Fortanix®

DATA SHEET

Amazon Web Services (AWS) Cloud Key Management with Fortanix

Full control over your AWS cloud keys with Fortanix Data Security Manager

Overview

Like most other cloud service providers, Amazon Web Services (AWS) offer their own cloud-native key management service to generate and manage master keys. But the native key management comes with its own shortcomings.
Some of the drawbacks are as follows:

- The cloud provider owns the key material, and the key can only be used in one cloud and typically for a single tenant.
- If a master key is deleted, then there is no way to get that key back. Any data encrypted under that key is lost.
- No consistent way of setting fine-grained controls over key management policies across multi-cloud. Customers do not get a single pane of glass for multi-geo and multi-cloud key management. The policy framework and auditing will be different for every cloud.

Solution Overview

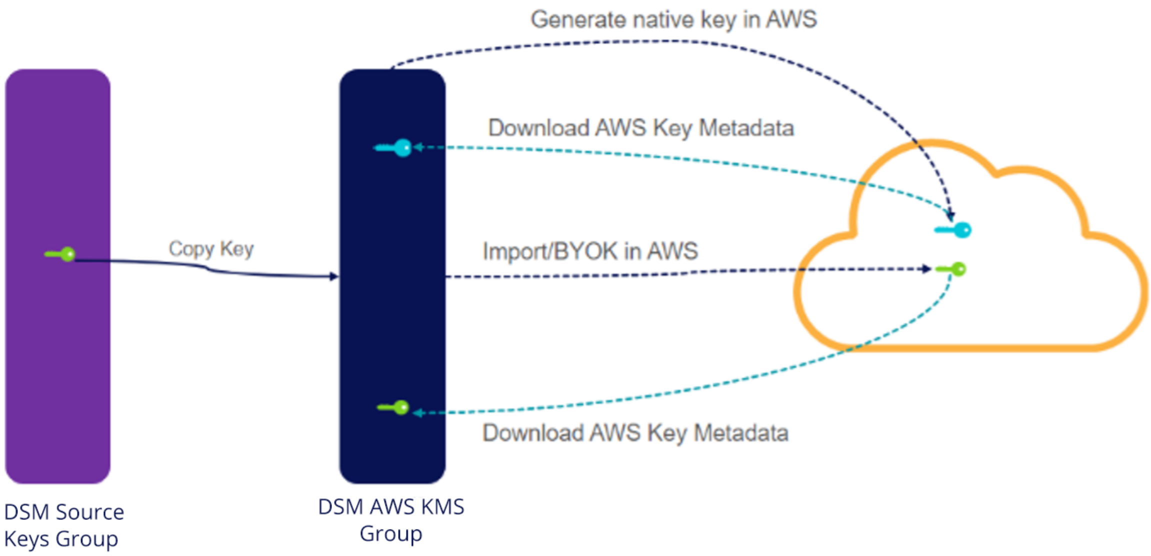
The Fortanix solution for AWS Key Management offers complete automated Bring Your Own Key (BYOK) and lifecycle management for management and automation of native AWS KMS keys (CMK – Customer Master Key) and allows users to manage all keys centrally and securely.

This enables AWS users to bring or import their own master key, which AWS stores in their key management system and encrypts all Data Encryption Keys (DEKs) under that key—providing greater control over their data and keys.

Why Fortanix?

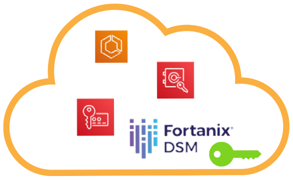
	AWS Native Customer Master Key Management	Fortanix Bring Your Own Key solution for AWS
Key generation	Key material is owned and generated by AWS KMS.	Key material is owned and generated in the customer- owned external KMS/ HSM.
Key control	Key material belongs to AWS KMS and cannot be exported by the customers.	Key material belongs to the customer and can be exported if needed.
Multi- region/ tenant support	Key material is unique to one region and account.	Key material is unique, however, can exist in more than one region and/or AWS accounts concurrently.
Disaster recovery	To pull a kill switch, the key will need to be permanently deleted, but then it cannot be restored.	To pull a kill switch, only the key material can be deleted, but then it can be restored on-demand.

Fortanix Data Security Manager allows organizations to Bring Your Own Key (BYOK) for AWS cloud. With this approach customers bring or import their own master key, which AWS stores in their key management system and encrypts all Data Encryption Keys (DEKs) under that key. This provides customers with greater control over their data and keys.

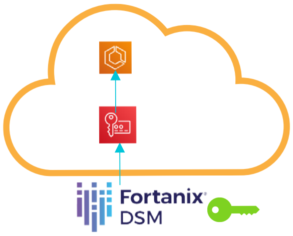

Generate native key in AWS
Download AWS Key Metadata
Copy Key
Import/BYOK in AWS
Download AWS Key Metadata
DSM Source Keys Group
DSM AWS KMS Group

Fortanix DSM Use Cases for AWS

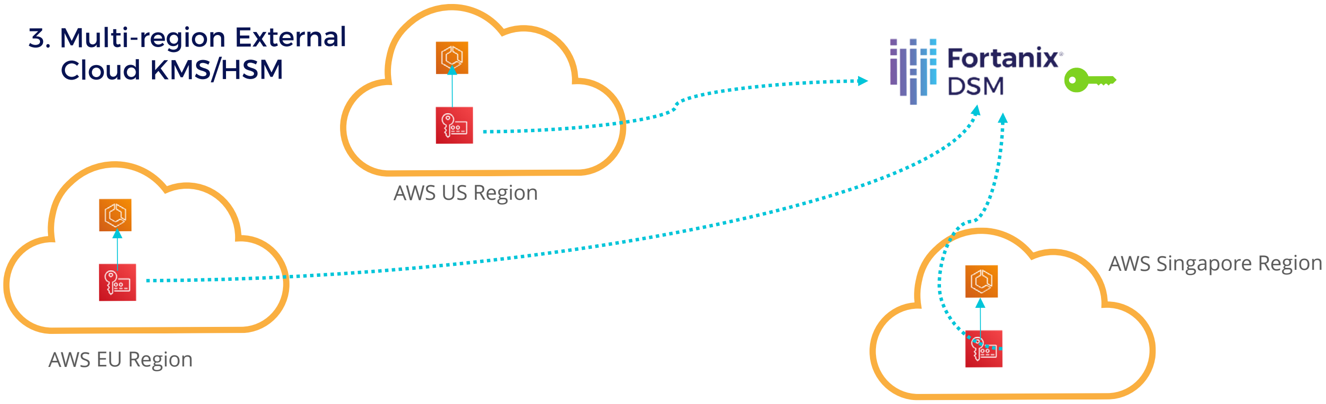
1. Native KMS on AWS



2. Automatic BYOK with Fortanix DSM as External KMS + FIPS 140-2 Level 3HSM



3. Multi-region External Cloud KMS/HSM



Key Benefits

GET FULL CONTROL OVER KEYS

Customers can bring or import a master key which the AWS stores within its KMS. This allows customers to retain ownership of the master key material and have greater control over the data stored in AWS.

EASILY MANAGE AWS KEY STATES AND OPERATIONS

Fortanix helps customers easily manage the AWS key states and operations as the same nomenclature of AWS KMS is used in Fortanix AWS KMS integrations. Also, a customer can author AWS key policies from Fortanix.

STOP DATA BREACHES WITH KILL -SWITCH

Gives you a central kill -switch and a fully managed disaster recovery for all your keys. Key material can be deleted from Fortanix to make an AWS key in “Pending Import” state and stop data breaches. Key material can also be reclaimed by importing it back into the cloud KMS.

SECURE DATA ACROSS LOCATIONS AND REGIONS

Offers greater flexibility as the same keys can be used to secure data across multiple accounts, locations, and regions.

MANAGE MULTI-CLOUD KEYS FROM A SINGLE PANE

Fortanix Data Security Manager allows you to manage and control multi-cloud keys in a completely cloud agnostic way. Organizations can keep full custody of their keys in a FIPS 140-2 level 3 certified HSM.

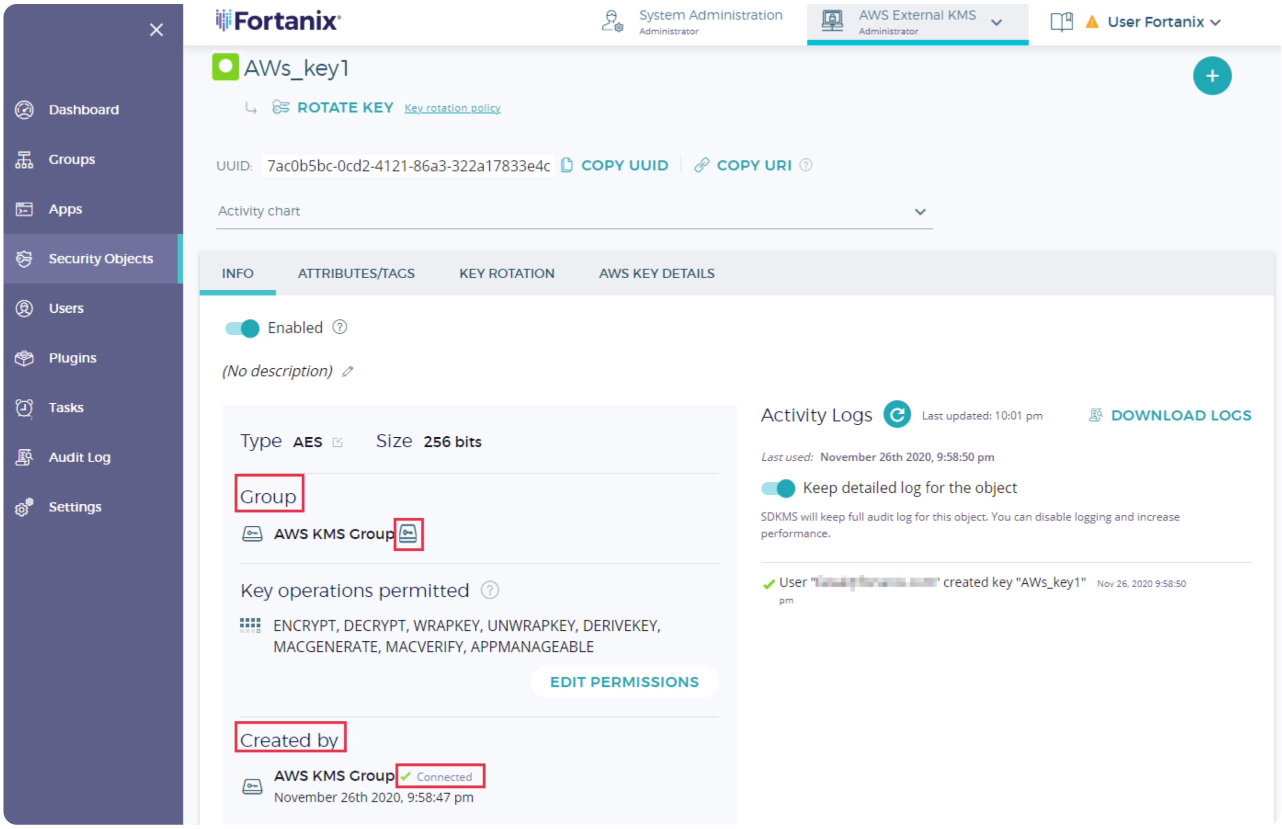
GET CENTRALIZED CONTROL AND AUDIT OF KEYS.

Fortanix Data Security Manager enables organizations to apply central control and audit the keys using quorum approvals and audit logs.

How does the Solution Work?

An AWS KMS group is created in the Fortanix DSM account, and this group is configured to interact with the AWS KMS.

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



AWs_key1

UUID: 7ac0b5bc-0cd2-4121-86a3-322a17833e4c

Enabled

(No description)

Type AES Size 256 bits

Group

AWS KMS Group

Key operations permitted

ENCRYPT, DECRYPT, WRAPKEY, UNWRAPKEY, DERIVEKEY, MACGENERATE, MACVERIFY, APPMANAGEABLE

Created by

AWS KMS Group ✓ Connected
November 26th 2020, 9:58:47 pm

Activity Logs Last updated: 10:01 pm

Last used: November 26th 2020, 9:58:50 pm

Keep detailed log for the object

SDKMS will keep full audit log for this object. You can disable logging and increase performance.

✓ User "[redacted]" created key "AWs_key1" Nov 26, 2020 9:58:50 pm