

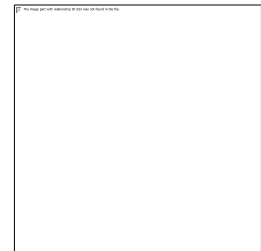


## AWS Key Management Service (KMS) & CloudHSM

Amazon Web Services

# AWS Key Management Service (KMS)

AWS Key Management Service (KMS) makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.



AWS Key Management  
Service

# AWS Key Management Service (KMS)

Fully Managed

Centralized Key  
Management

Managed Encryption of  
AWS services

Encrypt Data in  
your Applications

Build in Auditing

Secure

Compliance

# Amazon CloudHSM

Amazon Hardware Security Module (HSM) is a cloud service that uses dedicated HSM appliances within the AWS Cloud to help you design and deploy stringent data security solutions which meet regulatory and compliance requirements. The hardware appliance is designed to provide a secure key storage and cryptographic solution which involves utilizing tamper-proof hardware modules and enables you to use the key material without exposing it to anyone else. You are in complete control of access to the cryptographic keys that can then be used to encrypt and decrypt data. Amazon manages and maintains the hardware but does not have access to your keys.



# Amazon CloudHSM

You should consider using AWS CloudHSM if you require:

- Keys stored in dedicated, third-party validated hardware security modules under your exclusive control. You can develop applications and integrate them with CloudHSM, and use third-party encryption solutions available from AWS Technology Partners. Examples include EBS volume encryption and S3 object encryption and key management.
- FIPS 140-2 compliance.
- Integration with applications using PKCS#11, Java JCE, or Microsoft CNG interfaces.
- High-performance in-VPC cryptographic acceleration (bulk crypto).

# CloudHSM vs. AWS KMS

AWS Key Management Service (KMS) is a multi-tenant, managed service that allows you to use and manage encryption keys. However, AWS CloudHSM provides a dedicated, FIPS 140-2 Level 3 HSM under your exclusive control, directly in your Amazon Virtual Private Cloud (VPC).

# Next Video

Amazon Macie