General

Q: What is AWS Key Management Service (KMS)?
AWS KMS is a managed encryption service that enables you to easily encrypt your data. AWS KMS provides a highly available key storage, management, and auditing solution for you to encrypt your data across AWS services and within your own applications.

Q: Why should I use AWS KMS?
If you are a developer who needs to encrypt data in your applications, you should use the AWS SDKs with AWS KMS support to easily use and protect encryption keys. If you're an IT administrator looking for a scalable key management infrastructure to support your developers and their growing number of applications, you should use AWS KMS to reduce your licensing costs and operational burden. If you're responsible for proving data security for regulatory or compliance purposes, you should use AWS KMS to verify that data is encrypted consistently across the applications where it is used and stored.

Q: How do I get started with AWS KMS?
The easiest way is to get started using AWS KMS is to check the box to encrypt your data within supported AWS services and use the default keys that are created in your account for each service. If you want further controls over the management of these keys, you can create keys in AWS KMS and assign them to be used in the supported AWS services when creating encrypted resources as well as use them directly within your own applications. AWS KMS can be accessed from the "Encryption Keys" section of the AWS Identity and Access Management (IAM) console for web-based access, and the AWS KMS Command Line Interface or AWS Software Development Kit for programmatic access. Visit the Getting Started page to learn more.

- Re-enable disabled keys
- Delete keys that you no longer use
- Audit use of keys by inspecting logs in AWS CloudTrail

Q: How does AWS KMS work?
AWS KMS allows you to centrally manage and securely store your keys. You can generate keys in AWS KMS or import them from your key management infrastructure. These keys can be used from within your applications and supported AWS services to protect your data, but the key never leaves AWS KMS. You submit data to AWS KMS to be encrypted, or decrypted, under keys that you control. You set usage policies on these keys that determine which users can use them to encrypt and decrypt data. All requests to use these keys are logged in AWS CloudTrail so you can understand who used which key when.

Q: Where is my data encrypted if I use AWS KMS?
You can use AWS KMS to help encrypt data locally in your own applications or have it encrypted within a supported AWS service. You can use an AWS SDK with AWS KMS support to do the encryption wherever your applications run. You can also request a supported AWS service to encrypt your data as it is being stored. AWS CloudTrail provides access logs to allow you to audit how your keys were used in either situation.

Q: Which AWS cloud services are integrated with AWS KMS?
AWS KMS is seamlessly integrated with several other AWS services to make encrypting data in those services as easy as checking a box and selecting the master key you want to use. See the Features page for the list of AWS services currently integrated with AWS KMS. All use of your keys

While AWS KMS does support sending data less than 4 KB to be encrypted, envelope encryption can offer significant performance benefits. When you encrypt data directly with AWS KMS it must be transferred over the network. Envelope encryption reduces the network load for your application or AWS cloud service. Only the request and fulfillment of the data key through AWS KMS must go over the network. Since the data key is always stored in encrypted form, it is easy and safe to distribute that key where you need it to go without worrying about it being exposed. Encrypted data keys are sent to AWS KMS and decrypted under master keys to ultimately allow you to decrypt your data. The data key is available directly in your application without having to send the entire block of data to AWS KMS and suffer network latency.

Q: What's the difference between a key I create vs. default master keys created for me for use within AWS cloud services?

You have the option of selecting a specific master key to use when you want an AWS service to encrypt data on your behalf. A default master key specific to each service is created in your account as a convenience the first time you try to create an encrypted resource. This key is managed by AWS KMS but you can always audit its use in AWS CloudTrail. You can alternately create a customer master key in AWS KMS that you can then use in your own applications or from within a supported AWS service. AWS will update the policies on default master keys as needed to enable new features in supported services automatically. AWS does not modify policies on keys you create.

Q: Why should I create a customer master key?

Creating a key in AWS KMS gives you more control than you have with default service master keys. When you create a customer master key, you can choose to use key material generated by AWS KMS on your behalf or import your own key material, define an alias, a description, and opt-in to have the key automatically rotated once per year if it backed by key material generated by AWS KMS. You also can define permissions on the key to control who can use and manage the key. Management and usage activity related to the key is available for audit in AWS CloudTrail.

Q: How is the key that I import into AWS KMS protected in transit?
During the import, your key must be wrapped by a AWS KMS-provided public key using one of the two RSA PKCS#1 schemes. This ensures that your encrypted key can only be decrypted by AWS KMS.

Q: What's the difference between a key I import vs. a key generated for me by AWS KMS?
There are two main differences between a key that you import vs. a key created for you by AWS KMS:

1. You must securely maintain a copy of your imported keys in your key management infrastructure so that you can re-import them at any time. AWS ensures the availability, security, and durability of keys generated by AWS KMS on your behalf until you schedule the keys for deletion.
2. You may set an expiration period for an imported key to automatically delete the key from AWS KMS after the expiration period. You may also delete an imported key on demand without deleting the underlying customer master key. Further, you can manually disable or delete a customer master key with an imported key at any time. A key generated by AWS KMS can only be disabled or scheduled for deletion, it cannot have an expiration time placed on it.

Q: Can I rotate my keys?
Yes. You can choose to have AWS KMS automatically rotate keys generated by AWS KMS on your behalf every year. Automatic key rotation is not supported for imported keys. If you choose to import keys to AWS KMS, you can manually rotate them whenever you want.

Q: Do I have to re-encrypt my data after keys in AWS KMS are rotated?
If you choose to have AWS KMS automatically rotate keys generated by AWS KMS on your behalf, you don't have to re-encrypt your data. AWS KMS keeps previous versions of keys to use for

deletion. Once a key gets deleted, you can no longer use it. All data protected under a deleted master key is inaccessible.

For customer master keys with imported key material, you can delete the key material without deleting the customer master key id or metadata in two ways. First, you can delete your imported key material on demand without a waiting period. Second, at the time of importing the key material into the customer master key, you may define an expiration time for how long AWS can use your imported key material before it is deleted. You can re-import your key material into the customer master key if you need to use it again.

Q: What should I do if my imported key material has expired or I accidentally deleted it?
You can re-import your copy of the key material with a valid expiration period to AWS KMS under the original customer master key so it can be used.

Q: Can I be alerted that I need to re-import the key?
Yes. Once you import your key to a customer master key, you will receive an Amazon CloudWatch Metric every few minutes that counts down the time to expiration of the imported key. You will also receive an Amazon CloudWatch Event once the imported key under your customer master key expires. You can build logic that acts on these metrics or events and automatically re-imports the key with a new expiration period to avoid an availability risk.

Q: Can I use AWS KMS to help manage encryption of data outside of AWS cloud services?
Yes. AWS KMS is supported in AWS SDKs, AWS Encryption SDK, and the Amazon S3 Encryption Client to facilitate encryption of data within your own applications wherever they run. AWS SDK in the Java, Ruby, .NET, and PHP platforms support AWS KMS APIs. Visit the Developing on AWS website for more information.

With AWS KMS, you pay only for what you use, there is no minimum fee. There are no set-up fees or commitments to begin using the service. At the end of the month, your credit card will automatically be charged for that month's usage.

You are charged for all customer master keys you create, and for API requests made to the service each month above a free tier.

For current pricing information, please visit the AWS KMS pricing page.

Q: Is there a free tier?
Yes. With the AWS Free Usage Tier you can get started with AWS KMS for free in all regions. Default master keys created on your behalf are free to store in your account. There is a free tier for usage as well that provides a free number of requests to AWS KMS each month. For current information on pricing, including the free tier, please visit the AWS KMS pricing page.

Q: Do your prices include taxes?
Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales tax. For customers with a Japanese billing address, use of AWS services is subject to Japanese Consumption Tax. You can learn more here.

Security

Q: Who can use and manage my keys in AWS KMS?
AWS KMS enforces usage and management policies that you define. You choose to allow AWS

More details about these security controls can be found in the AWS KMS Cryptographic Details whitepaper. You can also review the FIPS 140-2 certificate for AWS KMS HSM along with the associated Security Policy to get more details about how AWS KMS HSM meets the security requirements of FIPS 140-2. In addition, you can download a copy of the Service Organization Controls (SOC) report from AWS Artifact to learn more about security controls used by AWS KMS to protect your master keys.

Q: How do I migrate my existing AWS KMS master keys to use FIPS 140-2 validated HSMs?
All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated HSMs. No action is required on your end to use the FIPS 140-2 validated HSMs.

Q: Which AWS regions have FIPS 140-2 validated HSMs?
FIPS 140-2 validated HSMs are available in all AWS regions where AWS KMS is offered.

Q: What is included in the FIPS 140-2 validation for AWS KMS HSMs?
Details about this validation can be found in the FIPS 140-2 certificate for AWS KMS HSM along with the associated Security Policy.

Q: What is the difference between the FIPS 140-2 validated endpoints and the FIPS 140-2 validated HSMs in AWS KMS?
AWS KMS is a two-tier service. The API endpoints receive client requests over an HTTPS connection using only TLS ciphersuites that support perfect forward secrecy. These API endpoints authenticate and authorize the request before passing the request for a cryptographic operation to the AWS KMS HSMs.

For more details on PCI DSS compliant services in AWS, you can read the PCI DSS FAQs.

Q: How does AWS KMS secure the data keys I export and use in my application?
You can request that AWS KMS generate data keys that can be returned for use in your own application. The data keys are encrypted under a master key you define in AWS KMS so that you can safely store the encrypted data key along with your encrypted data. Your encrypted data key (and therefore your source data) can only be decrypted by users with permissions to use the original master key used in encrypting the data key.

Q: What length of keys does AWS KMS generate?
Master keys in AWS KMS are 256-bits in length. Data keys can be generated at 128-bit or 256-bit lengths and encrypted under a master key you define. AWS KMS also provides the ability to generate random data of any length you define suitable for cryptographic use.

Q: Can I export a master key from AWS KMS and use it in my own applications?
No. Master keys are created and used only within AWS KMS to help ensure their security, enable your policies to be consistently enforced, and provide a centralized log of their use.

Q: What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region.

Q: How can I tell who used or changed the configuration of my keys in AWS KMS?
Logs in AWS CloudTrail will show requests on your master keys, including both management requests (e.g. create, rotate, disable, policy edits) and cryptographic requests (e.g. encrypt/decrypt). Turn on AWS CloudTrail in your account to view these logs.

they get rotated, and who can manage them. AWS KMS integration with AWS CloudTrail gives you the ability to audit the use of your keys to support your regulatory and compliance activities. You interact with AWS KMS from your applications using the AWS SDK if you want to call the service APIs directly, or the AWS Encryption SDK if you want to perform client-side encryption.

Learn more about pricing

See pricing examples, calculate your costs.

Learn more »

Sign up for a free account

Instantly get access to the AWS Free Tier.

Sign up »

Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.