What is AWS Secrets Manager?

PDF | RSS

AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, application credentials, OAuth tokens, API keys, and other secrets throughout their lifecycles. Many AWS services store and use secrets in Secrets Manager.

Secrets Manager helps you improve your security posture, because you no longer need hard-coded credentials in application source code. Storing the credentials in Secrets Manager helps avoid possible compromise by anyone who can inspect your application or the components. You replace hard-coded credentials with a runtime call to the Secrets Manager service to retrieve credentials dynamically when you need them.

With Secrets Manager, you can configure an automatic rotation schedule for your secrets. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise. Since the credentials are no longer stored with the application, rotating credentials no longer requires updating your applications and deploying changes to application clients.

For other types of secrets you might have in your organization:

- AWS credentials – We recommend AWS Identity and Access Management.
- Encryption keys – We recommend AWS Key Management Service.
- SSH keys – We recommend Amazon EC2 Instance Connect.
- Private keys and certificates – We recommend AWS Certificate Manager.

Get started with Secrets Manager

If you are new to Secrets Manager, start with one of the following tutorials:

- Move hardcoded secrets to AWS Secrets Manager
- Move hardcoded database credentials to AWS Secrets Manager
- Set up alternating users rotation for AWS Secrets Manager
- Set up single user rotation for AWS Secrets Manager

Other tasks you can do with secrets:

- Manage secrets
- Control access to your secrets
- Get secrets
- Rotate secrets
- Monitor secrets
- Monitor secrets for compliance
- Create secrets in AWS CloudFormation

Compliance with standards

AWS Secrets Manager has undergone auditing for the multiple standards and can be part of your solution when you need to obtain compliance certification. For more information, see Compliance validation for AWS Secrets Manager.

Pricing

When you use Secrets Manager, you pay only for what you use, with no minimum or setup fees. There is no charge for secrets that are marked for deletion. For the current complete pricing list, see AWS Secrets Manager Pricing. To monitor your costs, see Monitor Secrets Manager costs.

You can use the AWS managed key `aws/secretsmanager` that Secrets Manager creates to encrypt your secrets for free. If you create your own KMS keys to encrypt your secrets, AWS charges you at the current AWS KMS rate. For more information, see AWS Key Management Service Pricing.

When you turn on automatic rotation (except managed rotation), Secrets Manager uses an AWS Lambda function to rotate the secret, and you are charged for the rotation function at the current Lambda rate. For more information, see AWS Lambda Pricing.

If you enable AWS CloudTrail on your account, you can obtain logs of the API calls that Secrets Manager sends out. Secrets Manager logs all events as management events. AWS CloudTrail stores the first copy of all management events for free. However, you can incur charges for Amazon S3 for log storage and for Amazon SNS if you enable notification. Also, if you set up additional trails, the additional copies of management events can incur costs. For more information, see AWS CloudTrail pricing.

View related pages *Abstracts generated by AI*

Dms › sbs
Step 4: Store Database Credentials in AWS Secrets Manager
Store database credentials in AWS Secrets Manager, connect to source and target databases, create migration project
January 25, 2024

Dms › sbs
Step 4: Store Database Credentials in AWS Secrets Manager
Store database credentials in AWS Secrets Manager, connect to source and target databases, create migration project
July 28, 2024

Wellarchitected › security-pillar
SEC02-BP03 Store and use secrets securely
January 25, 2024

1 2 3

Discover highly rated pages *Abstracts generated by AI*

Secretsmanager › userguide
Use AWS Secrets Manager secrets in Amazon Elastic Kubernetes Service
Use AWS Secrets Manager secrets in Amazon EKS pods with AWS Secrets and Configuration Provider, set up access control, identify secrets to mount, troubleshoot mounted secrets.
July 19, 2024

Secretsmanager › userguide
Rotate AWS Secrets Manager secrets
Secrets Manager enables periodic secret rotation, updating credentials in secrets and databases. Managed rotation configures rotation automatically, while Lambda functions update other secret types.
April 19, 2024

Secretsmanager › userguide
Manage secrets with AWS Secrets Manager
Manage AWS Secrets Manager secrets lifecycle, rotation, retrieval, security
September 10, 2024

1 2