

To create secrets in AWS Secrets Manager manually using the AWS Management Console, follow these steps:

1.Open the AWS Management Console: Go to the AWS Management Console (<https://console.aws.amazon.com>) and sign in to your AWS account.

Navigate to AWS Secrets Manager: Use the search bar at the top of the console or locate the "Security, Identity & Compliance" category and click on "Secrets Manager".

Click on "Store a new secret": On the Secrets Manager dashboard, click on the "Store a new secret" button.



2.Choose the type of secret: Select the type of secret you want to create. You can choose between "Credentials for RDS database", "Credentials for Redshift database", "Credentials for DocumentDB database", "Credentials for MySQL database", "Other type of secrets (e.g., API key, SSH key)", and "Plaintext".

The screenshot shows the 'Choose secret type' form in the AWS console. It has a title 'Choose secret type' and a sub-header 'Secret type Info'. There are five radio button options arranged in two rows. The first option, 'Credentials for Amazon RDS database', is selected and highlighted with a blue border. An arrow points to this option from the text in the next step. The other options are 'Credentials for Amazon DocumentDB database', 'Credentials for Amazon Redshift cluster', 'Credentials for other database', and 'Other type of secret API key, OAuth token, other.'.

3.Enter the secret details: Fill in the necessary information based on the type of secret you selected. The required information may vary depending on the secret type. For example, if you choose "Plaintext", you will only need to enter the secret value. If you choose a database-specific secret, you will need to provide the connection details and credentials.

The screenshot shows the 'Credentials' form, which is part of the secret creation process for a database-specific secret. It has a title 'Credentials Info'. There are two text input fields: 'User name' and 'Password'. Both fields contain redacted text. Below the password field is a checkbox labeled 'Show password' which is checked.

For database you have to choose database for which you want to store the credentials and then click on next

Encryption key [Info](#)
You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager

↻

[Add new key](#)

Database [Info](#)

Q Search instances

< 1 >

DB instance	DB engine	Status	Creation date (UTC)
organisation	mysql	available	May 24, 2023 at 09:...

Cancel

Next

4.Configure the secret: Give the name for the secret and remaining all are optional and then click on next

Configure secret

Secret name and description [Info](#)

Secret name

A descriptive name that helps you find your secret later.

dummy-db

Secret name must contain only alphanumeric characters and the characters /_+-.@-

Description - optional

access mysql database for the instance

Maximum 250 characters.

Tags - optional

No tags associated with the secret.

Add

Resource permissions - optional [Info](#)

Add or edit a resource policy to access secrets across AWS accounts.

Edit permissions

Replicate secret - optional

Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

Cancel

Previous

Next

5.Review and create the secret: Verify the information you provided and click on the "Next" button. Review the settings once more on the next screen, and if everything is correct, click on the "Store" button to create the secret.

🔔 You successfully stored the secret dummy-db. To show it in the list, choose Refresh. Use the sample code to update your applications to retrieve this secret.

[View details](#)

AWS Secrets Manager > Secrets

Secrets

↻

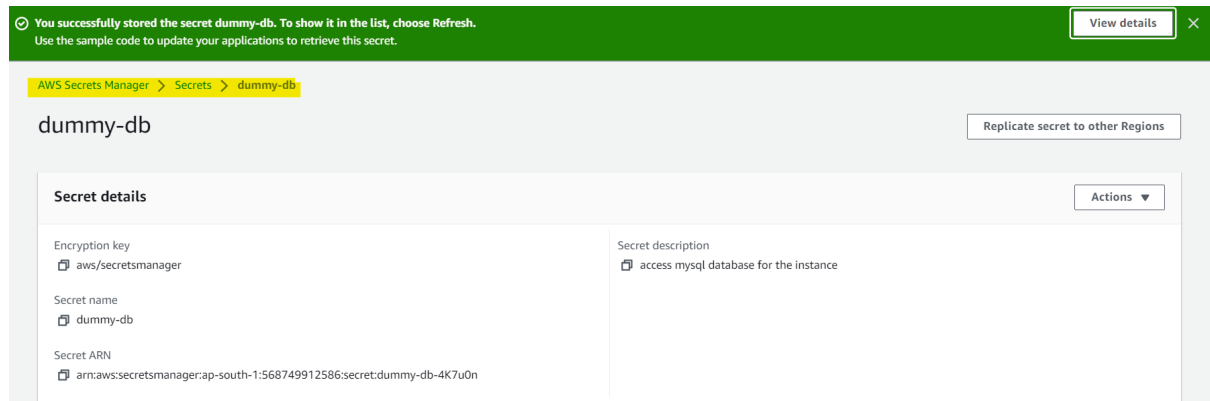
Store a new secret

Q Filter secrets by name, description, tag key, tag value, owning service or primary Region

< 1 > ⚙

Secret name	Description	Last retrieved (UTC)
database	-	May 24, 2023

6. Verify the secret creation: Once the secret is created, you will be redirected to the secret details page. Here, you can view the secret ARN, version history, and other relevant information.



That's it! You have now manually created a secret in AWS Secrets Manager using the AWS Management Console. You can access and manage the secret from the console or retrieve its value programmatically using its ARN or alias and also it will give some programs to retrieve the data.