

Secrets Manager

Getting Started

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Getting Started

Last updated : 2020-11-16 11:19:10

You can use Secrets Manager (SSM) to centrally retrieve, manage, and store different types of secrets, including encrypted database credentials, API keys, other keys, and sensitive configuration. SSM enables you to effectively avoid plaintext leakage caused by hardcoding and business risks caused by out-of-control permissions.

Step 1: Sign up

Sign up for a Tencent Cloud account and complete the identity verification. For more information, please see [Signing up for a Tencent Cloud Account](#).

Step 2: Purchase SSM

Go to the [SSM Purchase Page](#), read and select the relevant billing description, and then click **Activate Now**.

Step 3. Perform operations in the console

After SSM is activated, you can go to the console and use SDK or CLI to create, store, delete, and manage secrets through their lifecycle.

Note :

- SSM depends on KMS to store encrypted sensitive secrets. Therefore, before using SSM, ensure that [KMS](#) is activated.
- To ensure that you can use SSM normally, please grant service role permissions of KMS to SSM. You can go to [CAM](#) to authorize SSM.