# Secrets Manager

# FAQs

# Product Documentation


©2013-2022 Tencent Cloud. All rights reserved.

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

Tencent Cloud

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.

# FAQs

Last updated：2020-11-16 14:08:30

### What is SSM?

Secrets Manager (SSM) is a management service that enables users to create, retrieve, update, and delete secrets through their lifecycle. You can use SSM together with resource-level role authorization and comprehensive audit control to centrally manage sensitive secrets easily.

### Why Tencent Cloud SSM?

SSM enables you to centrally retrieve, manage, encrypt, and store information such as database credentials, API keys, other keys, and sensitive configuration, avoiding plaintext leakage risks caused by hardcoding and business risks caused by out-of-control permissions.

### What is a secret?

A secret is the sensitive credential information (i.e., database credentials, account passwords, API keys, and SSH keys) used for identity verification of an application. You can use SSM to store various types of sensitive data, such as sensitive addresses and IP ports, as the secret content in the format of Name-Value pairs.

### Why should KMS be activated before activating SSM?

SSM uses the KMS-protected CMK as the encryption key, which can be the default CMK or the customized CMK, to centrally manage the keys of all types of applications. Therefore, you need to activate KMS before activating SSM.

### How do I connect my application to SSM?

Whether your application is in or outside Tencent Cloud, you can use the following two methods to connect it to SSM:

- Call SSM through the [SSM APIs or SDK].
- Use the SSM console to manage the lifecycle of secrets.

©2013-2022 Tencent Cloud. All rights reserved.