SSL Certificate Manager

Service Overview

Issue	11
Date	2020-08-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 What Is SSL Certificate Manager?

SSL Certificate Manager (SCM) allows you to purchase Secure Sockets Layer (SSL) certificates from the world's leading digital certificate authorities (CAs), upload existing SSL certificates, and centrally manage all your SSL certificates in one place.

SSL Certificates

An SSL certificate is an SSL-compliant digital certificate issued by a trusted CA.

After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.

An SSL certificate can:

- Authenticate websites and ensure that data is sent to the correct clients and servers.
- Set up encrypted connections between clients and servers, preventing data from being stolen or tampered with during transmission.

The SSL protocol specifies a mechanism for providing data security between application protocols (such as HTTP, Telnet, and FTP) and TCP/IP. It uses the public key technology to ensure security protocol above TCP/IP. It provides data encryption, server authentication, message integrity, and optional client authentication for TCP/IP connections. The SSL protocol solves the problem of insecure plaintext transmission on the Internet. The SSL protocol has become an international standard.

2 Functions

HUAWEI CLOUD SCM provides the following functions to help you implement HTTPS for websites and ensure secure access for websites:

- Uploading certificates

  You can upload a local certificate onto the SCM platform.

- Managing certificates

  You can change certificate names, edit certificate description, download certificates, and delete certificates.

- Pushing certificates

  You can push certificates to other HUAWEI CLOUD products in one click and deploy digital certificates at low costs.

3 Application Scenarios

You can obtain SSL certificates from the SCM and deploy them on websites, enterprise applications, or other services.

With these certificates deployed, HTTPS will be used to prevent the following risks:

- HTTP-compliant data is transmitted in plaintext between clients and servers, and therefore is prone to be intercepted or tampered with.
- Spoofing or phishing websites may exploit vulnerabilities in HTTP to steal user information or property.

The specific applications are as follows:

- Authenticating websites

  SCM provides SSL digital certificates to authenticate websites. This effectively prevents the websites from being forged.
- Authenticating applications

  SCM provides SSL digital certificate to authenticate cloud and mobile applications. For example, a wide range of cloud applications, such as CRM, OA, and ERP, can be authenticated to prevent unauthorized access.
- Protecting application data transmission

  SCM provides SSL digital certificates to encrypt data transmitted between websites/applications and clients. This effectively ensures data integrity and prevents data from being stolen or tampered with.

4 Product Advantages

SCM has the following advantages:

High security

SCM manages certificates and related information securely using Huawei's advanced high-security password solution. It also provides distributed storage and service architecture to ensure high reliability.

One-stop services

SCM lets you easily apply for, manage, query, and verify certificates for use with HUAWEI CLOUD services.

Flexible choice

A wealth of certificates issued by the world's leading digital CAs are available, such as OV, OV Pro, EV, EV Pro, DV, and DV (Basic) certificates. You can buy an SSL certificate based on your needs.

Professional and fast response

Professional personnel are always online and ready to answer any questions about certificate use. Certificates can be issued within 24 hours if information is complete and correct.

5 Permissions Management

If you need to assign different permissions to employees in your enterprise, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your HUAWEI CLOUD resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can assign permissions to allow some software developers to use SCM resources but disallow them to delete or perform any high-risk operations on resources.

If your HUAWEI CLOUD account does not require individual IAM users for permissions management, skip this section.

IAM is free. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

SCM Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit permissions from the groups to which they are added and perform specified operations on cloud services based on the permissions.

You can create IAM users in any region. SCM is a global service for all geographic regions. Therefore, SCM permissions are assigned to users in the Global project, and IAM users do not need to switch regions when accessing SCM.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Only a limited number of service-level roles for authorization are available. You need to also assign other dependent roles for the permission control to take effect. Roles are not ideal for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you

can grant SCM users only the permissions for managing a certain type of resources. Most policies define permissions based on APIs. For the API actions supported by SCM, see **Permissions Policies and Supported Actions**.

Table 5-1 lists all the system-defined roles and policies supported by SCM.

Table 5-1 System-defined roles and policies supported by SCM

Role/Policy Name	Description	Type	Dependency
SCM Administrator	SCM administrator permissions. Users with SCM administrator permissions have all the permissions for the SCM service.	System-defined role	The **Server Administrator** and **Tenant Guest** roles need to be assigned in the same project.
SCM FullAccess	All permissions for SCM	System-defined policy	None.
SCM ReadOnlyAccess	Read-only permission for SCM. Users with the read-only permission can only query certificate information but cannot add, delete, or modify certificates.	System-defined policy	None.

Table 5-2 lists the common operations for each system-defined policy or role of SCM. Select the policies or roles as required.

Table 5-2 Common operations for each system-defined policy or role of SCM

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
Querying the certificate list	Yes	Yes	Yes
Querying certificate details	Yes	Yes	Yes
Querying the product type of a certificate	Yes	Yes	Yes

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
Querying the product details of a certificate	Yes	Yes	Yes
Modifying a certificate	Yes	Yes	No
Deleting a certificate	Yes	Yes	No
Pushing a certificate	Yes	Yes	No
Querying push records	Yes	Yes	Yes
Uploading a certificate	Yes	No	No

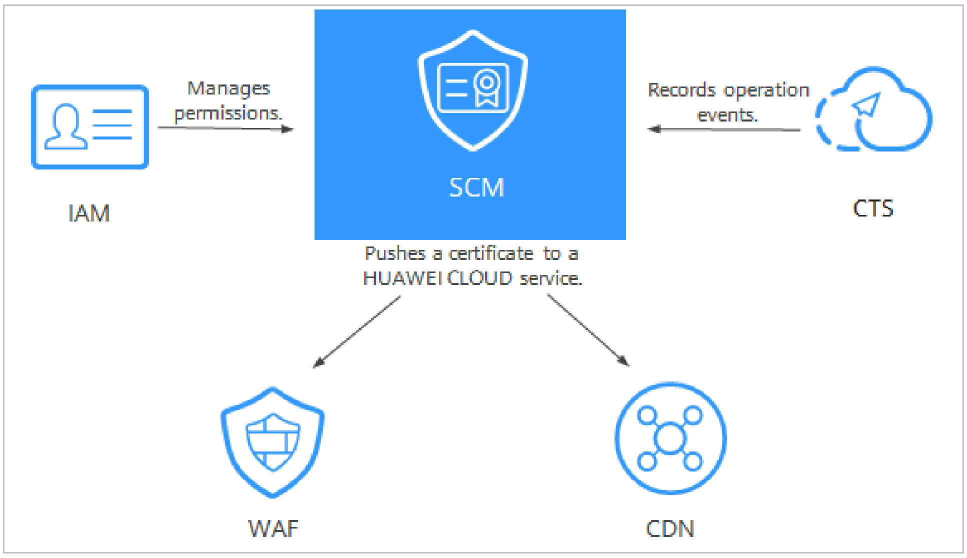
Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting SCM Permissions**
- **Supported Actions**

6 SCM and Other Services

Figure 6-1 describes the relationship between SCM and other cloud services.

Figure 6-1 Relationship between SCM and other cloud services


Manages permissions.
SCM
Records operation events.
IAM
CTS
Pushes a certificate to a HUAWEI CLOUD service.
WAF
CDN

WAF

You can purchase SSL certificates on the SCM console and deploy them on Web Application Firewall (WAF).

CDN

You can purchase SSL certificates on the SCM console and deploy them on Content Delivery Network (CDN).

CTS

Cloud Trace Service (CTS) provides you with a history of SCM operations. After enabling CTS, you can view generated traces to review and audit SCM operations. For details, see the *Cloud Trace Service User Guide*.

IAM

Identity and Access Management (IAM) provides the permission management for SCM.

Only users with the **SCM Administrator** permissions can use SCM.

To obtain the permissions, contact users with the **Security Administrator** permissions. For details, see *Identity and Access Management User Guide*.

7 Personal Data Protection

SCM encrypts personal data, such as the username, password, and phone number, to prevent leakage to unauthorized or unauthenticated entities or people.

Personal Data

Table 7-1 lists the personal data generated or collected by SCM.

Table 7-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Tenant ID	● Tenant ID in the token used when an operation is performed on the console. ● Tenant ID in the token used when an API is invoked.	No	Yes. The tenant ID is the certificate resource ID.
Contact name	Contact name entered when applying for a certificate.	Yes	Yes. The contact name is mandatory for manual verification.
Contact email address	Contact email address entered when applying for a certificate.	Yes	Yes. The contact email address is mandatory for manual verification.
Contact mobile number	Contact mobile number entered when applying for a certificate.	Yes	Yes. The contact person's mobile phone number is mandatory for manual verification.

Type	Collection Method	Can Be Modified	Mandatory
Enterprise's business license	When applying for a certificate, you can upload the enterprise's business license.	Yes	No
Bank account opening permit	You can upload the bank account opening permit when applying for a certificate.	Yes	No

Storage

SCM uses encryption algorithms to encrypt user data except for tenant IDs and stores encrypted data.

- Tenant IDs: Tenant IDs are not sensitive data and are stored in plaintext.
- Contact name, email address, phone number, enterprise's business license, and bank account opening permit: The data is stored after being encrypted.

Access Control

Token authentication is required for accessing personal data in the SCM database.

Logging

SCM logs all operations involving personal data, such as editing, querying, and deleting personal data. The logs are uploaded to Cloud Trace Service (CTS). You can view only the logs for your operations.

8 Basic Concepts

This section describes the concepts related to HUAWEI CLOUD SSL Certificate Manager (SCM).

Digital certificate

A digital certificate is a file digitally signed by a CA and contains information about the owner of a public key and the public key. It is a trusted certificate issued by an authority to a website. The simplest certificate contains a public key, name, and digital signature of the CA. Another important feature of a digital certificate is that it is valid only within a specific period of time.

SSL protocol

SSL is an encryption protocol that secures communication over a computer network. An encrypted channel can be established between the browser and website to prevent information from being stolen or tampered with during transmission.

CA

A CA is an authority responsible for issuing and managing digital certificates. As a trusted third party in e-commerce transactions, the CA verifies the validity of public keys in the public key system.

HTTPS

HTTPS, the secure version of HTTP, uses the SSL protocol to encrypt data before transmission. HTTPS activates an SSL encrypted channel between a web browser and a website server, allowing a user to securely visit the website where an SSL certificate has been installed. The channel allows high-strength bidirectional encrypted transmission to prevent leakage or tampering of the data being transmitted.

A Change History

Released On	Description
2020-04-28	This issue is the ninth official release. Changed certificate brand Symantec to DigiCert.
2020-02-10	This issue is the eighth official release. Changed SCM system-defined policies **SCM Admin** and **SCM Viewer** in **Permissions Management** into **SCM FullAccess** and **SCM ReadOnlyAccess**, respectively.
2020-01-20	This issue is the seventh official release. Updated the content in "Permissions Management" according to the changes on the IAM console.
2019-10-30	This issue is the sixth official release. Added **Personal Data Protection**.
2019-08-13	This issue is the fifth official release. Updated content in **What Is SSL Certificate Manager?**.
2019-05-21	This issue is the fourth official release. Modified content in **What Is SSL Certificate Manager?**.
2019-02-26	This issue is the third official release. Added the description of WAF in **SCM and Other Services**.
2019-01-18	This issue is the second official release. Optimized content in **What Is SSL Certificate Manager?**.
2018-08-10	This issue is the first official release.