Data Security Center

FAQs

Issue 11

Date 2022-09-22



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


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 Product Consulting....1
1.1 What is Data Security Center?....1
1.2 Does DSC Store My Data Assets or Files?....1
1.3 What Types of Unstructured Files Can DSC Parse?....1
2 Regions and AZs....7
2.1 What Are Regions and AZs?....7
2.2 Can DSC Be Used Across Regions?....8
3 Adding Data Assets....9
3.1 Agency Policies Obtained After the Access To Assets Is Allowed....9
3.2 How Do I Troubleshoot the Failure in Connecting to the Added Database?....10
4 Sensitive Data Identification and Masking....12
4.1 What Services Can Use DSC to Scan for Sensitive Data?....12
4.2 How Long Does It Take for DSC to Identify and Mask Sensitive Data?....13
4.3 Which Types of Sensitive Data Can Be Identified by DSC?....13
4.4 Does Data Masking Affect My Raw Data?....15
4.5 Does DSC Have Specific Requirements on the Character Set for Which Sensitive Data Is to Be Identified and Masked?....15
4.6 How Do I Add Multiple Identification Rule Groups?....15
5 Data Watermarking....17
5.1 Will the Source Data Be Modified During Data Watermarking?....17
5.2 Can the Watermark Be Extracted from a Damaged Document?....17
6 Data Usage Audit....18
6.1 Which Types of Abnormal Events Can Be Identified by DSC?....18
6.2 How Do I Audit DSC Operation Records?....19
7 Billing, Renewal, and Repurchase After Unsubscription....20
7.1 How Is DSC Billed?....20
7.2 How Do I Renew the Purchased DSC Before It Expires?....21
7.3 How Do I Unsubscribe from DSC?....22
A Change History....23

 Copyright © Huawei Technologies Co., Ltd.

1 Product Consulting

1.1 What is Data Security Center?

Data Security Center (DSC) is a latest-generation cloud data security management platform that protects your data assets by leveraging its data protection capabilities such as data classification, risk identification, data masking, and watermark-based source tracking. DSC gives you an insight into the security status of each stage in data security lifecycle and provides constant visibility of the security status of your data assets.

1.2 Does DSC Store My Data Assets or Files?

DSC does not store your data or files. DSC only identifies, anonymizes, or watermarks the data from the data sources you authorize DSC to access.

The data identification results are displayed on the DSC console. For details, see **Identification Results**.

1.3 What Types of Unstructured Files Can DSC Parse?

Table 1-1, **Table 1-2**, and **Table 1-3** list the types of unstructured files that can be parsed by DSC.

Table 1-1 Text and code files

No.	File Type	No.	File Type
1	Access database file	74	PDF document
2	ARFF file	75	Perl source code
3	ASP file	76	PGP file
4	ATOM file	77	PHP source code

Copyright © Huawei Technologies Co., Ltd.

No.	File Type	No.	File Type
5	BAT file	78	PKCS7 digital certificate file
6	BCPL source code	79	Plist file
7	BIB file	80	PostgreSQL database file
8	C# source code	81	PostScript document
9	C/C+ source code	82	PowerPoint document
10	CAD SldWorks file	83	Properties file
11	CAD document	84	Publisher file
12	CBOR file	85	Python source code
13	CFG file	86	Quattro-Pro spreadsheet
14	CHM file	87	Redis database file
15	Com executable file	88	RSS file
16	CSS file	89	RTF document
17	DataX configuration file	90	Ruby source code
18	DBF file	91	R source code
19	DIF file	92	SAS7BDAT file
20	DITA file	93	SAS file
21	Djvu Document	94	Scala source code
22	DOS executable file	95	Shell script
23	D source code	96	SQLite 3 database file
24	ELF executable file	97	SQLServer database file
25	EPUB eBook file	98	SQL source code
26	Excel document	99	SSH public key
27	FDF document	100	SSH configuration file
28	Fictionbook XML file	101	SSH private key
29	FTP session file	102	Staroffice document
30	GnucCash financial XML file	103	Swift source code
31	Go source code	104	TAB file

Copyright © Huawei Technologies Co., Ltd.

No.	File Type	No.	File Type
32	Groovy source code	105	TCL source code
33	HDR file	106	TEXT file
34	HOCON file	107	TFF file
35	HTML file	108	TNEF file
36	HTM file	109	Tomcat Application configuration file
37	HWP file	110	Tomcat Users configuration file
38	Ibooks file	111	Tomcat configuration file
39	Iis configuration file	112	TOML file
40	Initialization file	113	TSD file
41	ISA-Tab file	114	TSV file
42	iWork document	115	VCS file
43	Java Jce Keystore file	116	Visio document
44	Java Keystore file	117	Visual Basic source code
45	JavaScript source code	118	Virtual Reality Modeling Language (VRML) code
46	Java source code	119	Web Archive file
47	JSON file	120	WebLogic configuration file
48	JSP source code	121	WebVTT file
49	LaTeX source code	122	Windowsinf file
50	Log file	123	Windows full-text search index
51	Lua source code	124	Windows precompilation file
52	MariaDB database file	125	WordPerfect document
53	Markdown document	126	DOC file
54	Matlab source code	127	WPD document
55	Mbox file	128	WPS document
56	MIME HTML file	129	XDP file

 Copyright © Huawei Technologies Co., Ltd.

No.	File Type	No.	File Type
57	Microsoft Reader documentation	130	XFDF file
58	MongoDB database file	131	XHTML file
59	MRS configuration file	132	XLF file
60	Microsoft Works document	133	XLIFF file
61	MySQL database file	134	XLR file
62	NetCDF file	135	XLZ file
63	Objective-C source code	136	XML sitemap file
64	OBS configuration file	137	XML File
65	Office document	138	XMP file
66	OneNote file	139	XPS document
67	OpenDocument file	140	XPT file
68	OpenVPN configuration file	141	YAML file
69	Oracle database file	142	Common digital certificate files
70	Outlook file	143	Empty file
71	PASCAL source code	144	Configuration file **Windows Initialization**
72	PBM file	145	Other unencrypted text files
73	PCX file	146	Email document

Table 1-2 Compressed and binary files

No.	File Type	No.	File Type
1	7-Zip file	26	Lha compressed file
2	APK Android program	27	LZ4 compressed file
3	ARJ file	28	LZMA compressed file
4	AR file	29	MAT file

 Copyright © Huawei Technologies Co., Ltd.

No.	File Type	No.	File Type
5	BGP file	30	NetCDF file
6	Brotli compressed file	31	Object file
7	Bzip2 compressed file	32	Pack200 compressed file
8	Bzip compressed file	33	RAR compressed file
9	Cabinet compressed file	34	ShareLib file
10	Core dump file	35	Snappy compressed file
11	CPIO compressed file	36	TAR compressed file
12	Deflate64 compressed file	37	TCP dump file
13	DMG file	38	Tika-Unix-Dump file
14	ELF executable file	39	UNIX compressed file
15	GDAL file	40	Xcompress compressed file
16	GRB file	41	XLZ compressed file
17	GRIB2 file	42	XPI Firefox plug-in installation package
18	GRIB file	43	XZ compressed file
19	GZIP file	44	ZIP compressed file
20	HDF file	45	Zlib compressed file
21	HE5 file	46	ZSTD compressed file
22	ISO-19139 geographic information file	47	ZSTD dictionary file
23	ISO compressed file	48	Z compressed file
24	JAR file	49	Executable file
25	Java Class file	50	Common compressed file

Table 1-3 Images

No.	File Type	No.	File Type
1	BMP file	4	JFIF file

 Copyright © Huawei Technologies Co., Ltd.

No.	File Type	No.	File Type
2	PNM file	5	JPEG file
3	PNG file	6	TIFF file

 Copyright © Huawei Technologies Co., Ltd.

2 Regions and AZs

2.1 What Are Regions and AZs?

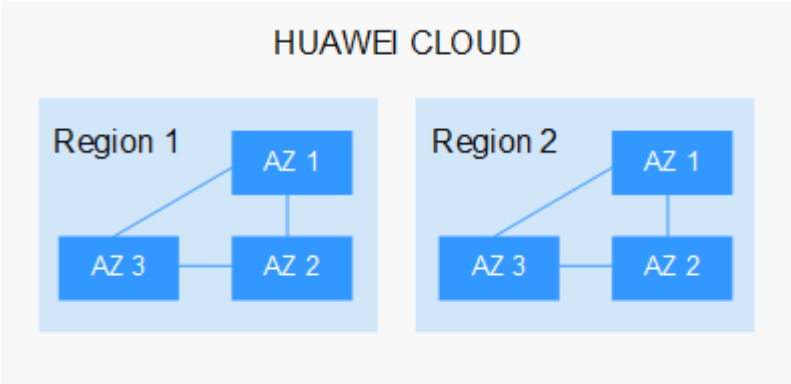
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



 Copyright © Huawei Technologies Co., Ltd.

HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2.2 Can DSC Be Used Across Regions?

DSC can only be used to identify and mask the sensitive data in resources of the region where DSC is located.

Copyright © Huawei Technologies Co., Ltd.

3 Adding Data Assets

3.1 Agency Policies Obtained After the Access To Assets Is Allowed

After the access to cloud resources is allowed, DSC can access your private OBS buckets, databases, big data assets, and data security overview. **Table 3-1** describes the agency policies obtained after the access is allowed.

Table 3-1 Agency policies

Asset	Policy	Scope	Remarks
OBS	OBS Adminstrator	Global	Used to configure OBS logs, obtain the OBS bucket list, and download items form OBS.
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
	OBS Adminstrator	Global	Used to obtain the logs delivered by OBS.
Database	ECS ReadOnlyAccess	Regional	Used to obtain the list of ECSs where databases are built.
	RDS ReadOnlyAccess	Regional	Used to obtain the RDS database list and related information.
	DWS ReadOnlyAccess	Regional	Used to obtain the DWS instance list.
	VPC FullAccess	Regional	Used to establish network connection and create VPC ports and security group rules
	KMS CMKFullAccess	Regional	Used to perform encryption using KMS in data masking.

 Copyright © Huawei Technologies Co., Ltd.

Asset	Policy	Scope	Remarks
Big Data	ECS ReadOnlyAccess	Regional	Used to obtain the list of ECSs where big data sources reside.
	CSS ReadOnlyAccess	Regional	Used to obtain the CSS data cluster list and data indexes.
	DLI Service User	Regional	Used to obtain the DLI queue and database.
	VPC FullAccess	Regional	Used to establish network connection and create VPC ports and security group rules.
	KMS CMKFullAccess	Regional	Used to perform encryption using KMS in data masking.
Overview	Tenant Guest	Regional	Used to obtain the list of cloud services used for data storage and processing.
	OBS Adminstrator	Global	Used to configure OBS logs, obtain the OBS bucket list, and download items form OBS.
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
	OBS Adminstrator	Global	Used for OBS to deliver logs.

3.2 How Do I Troubleshoot the Failure in Connecting to the Added Database?

DSC will check the connectivity of the added database. If the connection to the added database fails, perform the following operations to troubleshoot the problem:

Step 1 Check whether the IP address, account, password, and database name of the added database are correct.

- If no, correct it.
- If yes, go to **2**.

Step 2 Check whether all ports and protocols are bypassed in the outbound direction of the security group which the added database belongs.

- If no, add outbound rules for the security group. Add the database to DSC again after all ports and protocols are bypassed in the outbound direction of the security group. If the failure persists, go to **3**.
- If yes, go to **3**.

Step 3 Check whether the number of available IP addresses in the IP subnet corresponding to the database is 0.

 Copyright © Huawei Technologies Co., Ltd.

At least one IP address is required for DSC to establish connection to the added database. If the number of available IP addresses in the IP subnet corresponding to the database is 0, add available IP addresses to the database.

----End

 Copyright © Huawei Technologies Co., Ltd.

4 Sensitive Data Identification and Masking

4.1 What Services Can Use DSC to Scan for Sensitive Data?

DSC can scan data stored in OBS, RDS, CSS, DWS, or DLI for sensitive information by using built-in and custom rules.

The following table lists the data sources supported by DSC and identification restrictions.

Table 4-1 Supported data sources

Data Source	Data Type	Restriction
RDS	MySQL, SQL Server, and PostgreSQL	The first 500 lines of data records are sampled and scanned. The QPS reaches 300 times per second.
CSS	Big data asset	N/A
OBS	More than 200 file types	Files larger than 200 MB or encrypted files in the OBS bucket cannot be scanned.
DWS	N/A	N/A
ECS	Data in MySQL, SQL Server, PostgreSQL, and Oracle databases, as well as Elasticsearch instances	N/A
Data Lake Insight (DLI)	Big data asset	N/A

 Copyright © Huawei Technologies Co., Ltd.

4.2 How Long Does It Take for DSC to Identify and Mask Sensitive Data?

Identification Duration

The identification duration depends on the data volume, number of identification rules, and scan mode. The information provided in **Table 4-2** is for reference only.

Table 4-2 Identification duration

Data Source	Data Volume	Scan Mode	Duration (Minutes)
RDS	1,000 tables	Quick scan	5
CSS	10 million documents	Quick scan	15
OBS	100 MB	Quick scan	1
OBS	100 MB	Full scan	15

Data Masking Duration

DSC uses preset and customized masking algorithms to mask sensitive data stored in RDS and CSS. The following table describes the masking duration.

Table 4-3 Data masking duration

Data Source	Data Volume	Duration (Minutes)
RDS	10 million lines	40
CSS	10 million documents	40

4.3 Which Types of Sensitive Data Can Be Identified by DSC?

DSC can identify seven types of sensitive data, including sensitive images, personal data, and critical business information. The following table lists the types of sensitive data that can be identified by DSC.

 Copyright © Huawei Technologies Co., Ltd.

Table 4-4 Sensitive data types that can be identified by DSC

Type	Sensitive Data
Sensitive image	• ID card • Passport
Personal privacy	• ID card • Bank card • Name in Pinyin or English • Phone number • Email address • Passport No. • EEP • License plate No. • Phone number • Officer certificate • Gender • Vehicle identification number
Enterprise information	• Business license code • Tax registration certificate No. • Organization code of the enterprise • Unified social credit code
Key information	• PEM certificate • Private key • Access key ID • Secret access key • Hash password
Device information	• IP address • MAC address • JDBC URL • IPv6 address • IMEI • MEID
Location	• Province • City • GPS position • Address
Common information	Date

 Copyright © Huawei Technologies Co., Ltd.

4.4 Does Data Masking Affect My Raw Data?

No. The sensitive data masking function only reads data, masks sensitive information, and saves the data in a specified path without changing your raw data.

4.5 Does DSC Have Specific Requirements on the Character Set for Which Sensitive Data Is to Be Identified and Masked?

No.

For details about the data sources for which sensitive data can be identified by DSC, see **What Services Can Use DSC to Scan for Sensitive Data?**.

For details about the types of sensitive data can be identified by DSC, see **Which Types of Sensitive Data Can Be Identified by DSC?**.

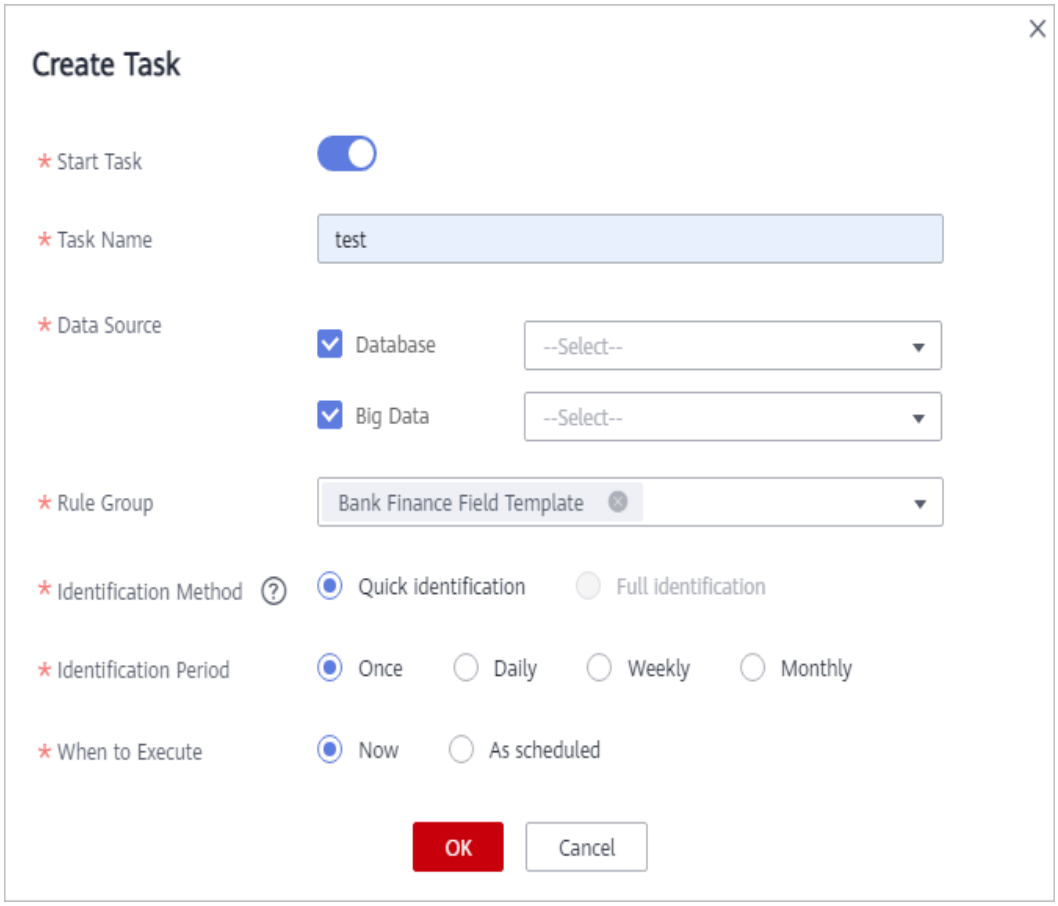
4.6 How Do I Add Multiple Identification Rule Groups?

DSC has over 100 sensitive data identification and masking rules for various scenarios and can identify and mask the sensitive information such as personal information (ID card information, bank card information, names, mobile numbers, email addresses, and more), enterprise information (business license numbers, tax registration certificate numbers, and more), and key information (PEM certificates, HEY private keys, and more), device information (IP addresses, MAC addresses, IPv6 addresses, and more), location information (provinces/states, cities, GPS locations, addresses, and more), and common information (dates and others). In addition, DSC supports custom identification rules. For details, see **Adding a Rule**.

When you create a scanning task for an asset, add multiple identification rule groups to add multiple rules, so you can configure multiple scanning tasks for the asset, as shown in **Figure 4-1**. For details, see **Creating a Sensitive Data Identification Task**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Creating a sensitive data identification task



 Copyright © Huawei Technologies Co., Ltd.

5 Data Watermarking

5.1 Will the Source Data Be Modified During Data Watermarking?

The source data will not be modified during data watermarking.

DSC injects watermarks into the files stored in the OBS bucket or local directory and generates the watermarked files. The files will be automatically downloaded to the directory specified, and there is no any modification to the source data. For details, see **Data Watermarking**.

5.2 Can the Watermark Be Extracted from a Damaged Document?

DSC data watermarking is highly robust. Watermarks are not easily removed during transmission or use. Even if the data carrier is tampered with or damaged, there is a high probability that watermarks are extracted.

- If several pages are deleted from a document, the watermarks can still be extracted.
- If an image is rotated, cropped, scaled, or retouched, the watermarks can still be extracted as long as the deformation is small.

 Copyright © Huawei Technologies Co., Ltd.

6 Data Usage Audit

6.1 Which Types of Abnormal Events Can Be Identified by DSC?

Currently, DSC can only identify abnormal events in OBS.

DSC identifies sensitive data based on its identification rules and monitors events related to the sensitive data. You can check results in the event list and handle the abnormal events as needed. **Table 6-1** lists the abnormal events that can be identified by DSC.

Table 6-1 Abnormal events that can be identified by DSC

Type	Event
Unauthorized data access	• Access sensitive files without granted permissions. • Download sensitive files.
Abnormal data operations	• Update sensitive files. • Append data to sensitive files. • Delete sensitive files. • Copy sensitive files.

 Copyright © Huawei Technologies Co., Ltd.

Type	Event
Abnormal data management	• When a bucket is added, the system detects that the bucket is a public read or a public read/write bucket. • When a bucket is added, the system detects that the access/ACL access permissions of a private bucket are granted for anonymous users or registered user groups. • The policy of a bucket containing sensitive files is changed or deleted. • The ACL of a bucket containing sensitive files is changed or deleted. • The cross-region replication configuration of a bucket containing sensitive files is modified or deleted. • The ACL of a sensitive file is modified or deleted.

Reference:

- **How Do I Handle Abnormal Events?**
- **How Do I View Abnormal Events?**

6.2 How Do I Audit DSC Operation Records?

All operations performed on DSC are recorded as API calls in CTS.

and you can view all the records on the CTS console for auditing. For details about how to view audit logs, see **Viewing Audit Logs**.

Copyright © Huawei Technologies Co., Ltd.

7 Billing, Renewal, and Repurchase After Unsubscription

7.1 How Is DSC Billed?

If you use DSC through the console, you will be billed on a yearly/monthly basis, which is prepaid. If you use DSC by APIs, including data masking and watermark APIs, you pay for what you used. DSC provides the standard and professional editions, and the database and OBS expansion packages.

Buy a required DSC edition and additional expansion packages based on your site requirements. You will be charged based on the selected billing items.

Billing Item

Table 7-1 Billing items

Billing Mode	Billing Item	Description
Yearly/Monthly	(Mandatory) Edition specifications	Billed based on the specifications of purchased DSC edition (standard or professional).
	(Optional) Database expansion package	Billed based on the number of purchased packages.
	(Optional) OBS expansion package	Billed based on the number of purchased packages.
	Required duration	Billed on a yearly or monthly basis.

Copyright © Huawei Technologies Co., Ltd.

Billing Mode	Billing Item	Description
Pay-Per-Use	APIs (data masking and watermarking)	APIs are included only in the professional edition. By default, the professional edition offers one million API calls each month. Note that the unused API calls for the previous month will become invalid. For pricing about extra API calls, see **Product Pricing Details**.

For price details, see **Product Pricing Details**.

7.2 How Do I Renew the Purchased DSC Before It Expires?

This section describes how to renew the DSC subscription before it expires. After the renewal, you can continue to use DSC.

Before your DSC subscription expires, the system will send an SMS message or email to remind you to renew it.

If you do not renew your subscription before it expires, a retention period will apply.

This period varies depending on your account. For details, see **Retention Period**.

To avoid unnecessary loss caused by security issues, renew your subscription before the retention period expires. If you do not renew the subscription, you cannot use DSC.

Procedure

Step 1 **Log in to the management console.**

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance** > **Data Security Center**.

Step 4 In the upper right corner, click **Renew**.

Step 5 On the renewal management page, complete the renewal.

For more details, see **Manually Renewing a Resource**.

----End

 Copyright © Huawei Technologies Co., Ltd.

7.3 How Do I Unsubscribe from DSC?

This section describes how to unsubscribe from DSC. To unsubscribe from an extension package, you must unsubscribe from both the purchased DSC edition and expansion package.

Procedure

Step 1 **Log in to the management console.**

Step 2 In the upper right part of the page, click **Billing Center**.

Step 3 In the navigation pane on the left, choose **Orders** > **Unsubscriptions and Returns/Exchanges**.

Step 4 Complete the unsubscription operations.

For more details, see **Unsubscription Rules**.

----End

Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2021-09-22	This issue is the eleventh official release. Modified **How Is DSC Billed?**.
2021-09-09	This issue is the tenth official release. • Modified **Does DSC Store My Data Assets or Files?**. • Added **Can the Watermark Be Extracted from a Damaged Document?**.
2021-09-02	This issue is the ninth official release. • Added **How Do I Add Multiple Identification Rule Groups?**. • Modified **What Are Regions and AZs?**.
2021-07-26	This issue is the eighth official release. Added **Will the Source Data Be Modified During Data Watermarking?**.
2021-05-27	This issue is the seventh official release. Added **Does DSC Have Specific Requirements on the Character Set for Which Sensitive Data Is to Be Identified and Masked?**.
2021-02-27	This issue is the sixth official release. Added the following FAQs: • **Can DSC Be Used Across Regions?** • **How Is DSC Billed?** • **How Do I Renew the Purchased DSC Before It Expires?** • **How Do I Unsubscribe from DSC?**

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2021-02-19	This issue is the fifth official release. Added **How Do I Troubleshoot the Failure in Connecting to the Added Database?**.
2021-02-07	This issue is the fourth official release. Added **Agency Policies Obtained After the Access To Assets Is Allowed**.
2021-01-26	This issue is the third official release. Added **What Types of Unstructured Files Can DSC Parse?**.
2020-11-16	This issue is the second official release. • Added **What Services Can Use DSC to Scan for Sensitive Data?**. • Added **How Long Does It Take for DSC to Identify and Mask Sensitive Data?**. • Added **Which Types of Abnormal Events Can Be Identified by DSC?**. • Added **Which Types of Sensitive Data Can Be Identified by DSC?**. • Added **Does DSC Store My Data Assets or Files?**. • Added **How Do I Audit DSC Operation Records?**. • Added **Does Data Masking Affect My Raw Data?**.
2020-09-30	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.