OceanStor Dorado 2000, Dorado 3000, Dorado 5000, and Dorado 6000 6.1.x

OceanStor Dorado 2000, 3000, 5000, and 6000 6.1.x Product Documentation

Issue Date 2022-12-20





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. 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

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129

People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

Contents	1
1 Configuring and Managing the Key Management Server (Utimaco, Applicable to 6.1.2 and Later)	2
1.1 About Utimaco Key Management Servers	2
1.2 Configuration Process	4
1.3 Hardware Deployment	4
1.4 Configuring the Key Management Server and Cluster	5
1.5 Connecting the Key Management Server to the Storage System	5
1.5.1 Generating and Exporting a Certificate on the Storage System	5
1.5.2 Signing the Certificate on a Key Management Server and Exporting the Certificate	6
1.5.3 Creating a Local User	8
1.5.4 Importing and Activating the Certificate on the Storage System	10
1.5.5 Configuring the External Key Service on the Storage System	11
1.6 Creating a Self-encrypting Storage Pool (Using SEDs)	12
1.7 Creating a Self-encrypting Storage Pool (Using the Data Encryption Function, Applicable to 6.1.5 and Later	
Versions)	15
1.7.1 Checking the License	15
1.7.2 Creating a Self-encrypting Storage Pool	15

1 Configuring and Managing the Key Management Server (Utimaco, Applicable to 6.1.2 and Later)

This chapter describes how to install and configure the Utimaco key management server.

About Utimaco Key Management Servers

Configuration Process

Hardware Deployment

Configuring the Key Management Server and Cluster

Connecting the Key Management Server to the Storage System

Creating a Self-encrypting Storage Pool (Using SEDs)

Creating a Self-encrypting Storage Pool (Using the Data Encryption Function, Applicable to 6.1.5 and Later Versions)

1.1 About Utimaco Key Management Servers

This section describes the network connection of the Utimaco key management server.

Typical Networking

A storage system connects to two Utimaco key management servers that are clustered in hot backup mode. <u>Figure</u> **1** shows the typical networking.

Figure 1 Typical networking of key management servers



Figure 2 shows port connections between different components.



To ensure that the key management servers can work properly, verify that the network communication between the following components is normal:

- Storage system's management network port -> key management servers' LAN1
- Maintenance terminal -> key management servers' LAN1
- Key management server 1's LAN1-> key management server 2's LAN1

• Backup server's network port -> key management servers' LAN1

1.2 Configuration Process

Before configuring key management servers, get familiar with the configuration procedure to ensure a successful deployment.

Figure 1 shows the procedure of configuring key management servers.

Figure 1 Configuration process



1.3 Hardware Deployment

This section describes how to install key management servers, connect their cables, and power on the servers.

Prerequisites

- The installation positions of the two key management servers have been determined.
- Cables and tools required for hardware installation have been prepared, including:
 - Serial cable (included in the product package)
 - Power cable (included in the product package)
 - Network cable (not included in the product package)
 - Phillips screwdriver (not included in the product package)
 - (Optional) USB-to-serial cable (not included in the product package)

D NOTE

Prepare the USB-to-serial cable if the maintenance terminal has no serial port.

Procedure

1. Determine the installation positions.

The key management servers must be installed on standard 19-inch racks. Determine proper positions on the rack to install the two key management servers. Ensure that there is enough space in front of and behind the servers for cable routing and connection, ventilation, and maintenance.

- 2. Wear ESD gloves and ESD wrist straps.
- 3. Unpack the key management server.
- 4. Install the key management server on the rack.
- 5. Use a network cable to connect the LAN1 port of the key management server to the management network port of the storage system through a switch.
- 6. Insert one end of the power cable to the electric socket at the server back, and insert the other end to the external AC power module.
- 7. Press the power switch on the front panel.
- 8. Put the baffle plate on the front panel, then insert and turn the key.
- 9. Repeat $\underline{3}$ to $\underline{8}$ to install and power on the other key management server.
- 10. If the maintenance terminal has no serial port, use the USB-to-serial cable to connect the USB port of the maintenance terminal to the serial port of the key management server.

1.4 Configuring the Key Management Server and Cluster

After hardware installation, initialize the key management server and create a cluster by following instructions in the server user guide and consulting the technical support engineer of the server manufacturer.

1.5 Connecting the Key Management Server to the Storage System

After the key management server cluster has been created, you must connect the key management servers to the storage system to provide the disk encryption service.

Generating and Exporting a Certificate on the Storage System

Signing the Certificate on a Key Management Server and Exporting the Certificate

Creating a Local User

Importing and Activating the Certificate on the Storage System

Configuring the External Key Service on the Storage System

1.5.1 Generating and Exporting a Certificate on the Storage System

This section describes how to generate and export a certificate required by the disk encryption function on the storage system.

Context

The certificate generated on the storage system is not signed. It must be signed on the key management server.

Procedure

- 1. Log in to DeviceManager.
- 2. Choose **Settings** > **Certificates**.
- 3. On the **Certificate Management** page, choose **KMC certificate**, and click **Export Request File**. On the displayed page, set the **Certificate Key Algorithm** to **RSA 2048** or **RSA 4096**, and then click **OK**.

D NOTE

You can also click **KMC certificate**. On the **Certificate Details** page that is displayed, click **Operation** > **Export Request File**, set the **Certificate Key Algorithm** to **RSA 2048** or **RSA 4096**, and then click **OK**.

1.5.2 Signing the Certificate on a Key Management Server and Exporting the Certificate

This section describes how to sign a key management server certificate and how to export the certificate. The certificate generated on the storage system must be signed on the key management server and saved properly. In addition, you must also export the CA certificate of the key management server.

Signing the Certificate

- 1. Log in to the key management server's web interface as an administrator.
- 2. Choose Security > Certificates & CAs > Local CAs.

The **Certificate and CA Configuration** interface is displayed, as shown in Figure 1.

Figure 1 CA certificate list

Help 🔸 Log Ou
vESKN Logged in as admi r
Help
CA Status
CA Certificate Active
Help

3. Select the default CA certificate and click Sign Request.

The Sign Certificate Request interface is displayed, as shown in Figure 2.

Figure 2 Sig	ning the certificate	
Home • Security •	Device	Help 🔸 Log Out
Keys & KMIP Objects Keys	Security / Local CAs Certificate and CA Configuration	vESKM Logged in as admin
Authorization Policies	Sign Certificate Request	Help
Users & Groups	Sign with Certificate Authority: ESKMCA (maximumdays) 🗸	
▶ LDAP	Certificate Purpose O Client	
Certificates & CAs Certificates	Certificate Duration (days):	
Trusted CA Lists	Certificate Request:	
Local CAs Known CAs		
Advanced Security + High Security		
SSL Options		

4. Set certificate request parameters.

SSH Options
FIPS Status Server

- a. Set Sign with Certificate Authority to ESKMCA (maximum xxxx days) (default value).
- b. Set Certificate Purpose to Client.

st Back

- c. Set **Certificate Duration (days)** to the validity period of the certificate. The value of this parameter must not be greater than **xxx** in **ESKMCA (maximum xxxx days)**.
- d. Copy the ***.csr** content of the certificate file exported from the storage system in Generating and Exporting a Certificate on the Storage System to the text box under **Certificate Request**.
- e. Click Sign Request.

The CA Certificate Information page is displayed, as shown in Figure 3.

nome accurry b	evice	Help 🔸 Log Out
Keys & KMIP Objects Keys KMIP Objects Authorization Policies	Security / Local CAs Certificate and CA Configuration	vESKM Logged in as admin
	CA Certificate Information	Help 🚷
Local Users & Groups	Key Size: 2048	
▶ LDAP	Start Date: Mar 2 09:10:07 2021 GMT Expiration: Jap 9 09:10:07 2031 GMT	
Certificates & CAs Certificates Trusted CA Lists Local CAs Known CAs	C: US ST: CA L: Campbell Issuer: C: Organization OU: Information Security OU: ESKMICcalCA emailAddress: infosec@organization.com	
Advanced Security High Security SSL Options 	C: CN Subject: O: Huawei OU: Storage CN: 2102351L/D10J8000007	
SSH Options FIPS Status Server	<pre>HIDDITCO.HIGANIEARISLA.URA HIMANA HIMAN</pre>	

Figure 3 CA certificate information

5. Click **Download** to export the signed certificate.

The signed certificate is named as **signed.crt**.

Exporting the CA Certificate

- 1. Log in to the key management server's web interface as an administrator.
- 2. Choose Security > Certificates & CAs > Local CAs.

The **Certificate and CA Configuration** interface is displayed, as shown in Figure 4.

Figure 4 CA certificate list

Home • Security •	Device			Help 🔸 Log Out
Keys & KMIP Objects Keys KMIP Objects Authorization Policies	Security / Local CAs Certificate and C	A Configuration		vESKM Logged in as admin
licers & Groups	Local Certificate Auth	ority List		Help 🗿
Local Users & Groups	CA Name CA In	formation	CA Status	
LDAP Certificates & CAs Certificates	ESKMCA Comi Essue Expir Edit Delete Download P	nor: ESKMLocalCA . Organization ss: Jan 9 17:26:47 2031 GMT operties Sign Request Show Signed Certs	CA Certificate Active	
Trusted CA Lists Local CAs	Create Local Certifica	te Authority		Help 💡
Known CAs	Certificate Authority Nar	e: ESKMCA		
Advanced Security	Common Nar	e: ESKMLocalCA	-	
High Security	Organization Nar	ne: Organization		
SSL Options	Organizational Unit Nar	ne: Information Security		
SSH Options	Locality Nar	ne: Campbell		
FIPS Status Server	State or Province Nar	ne: CA	-	
	Country Nar	ie: US		
	Email Addre	ss: infosec@organization.com	-	
	Algorith	m: RSA-2048 🗸		
	Certificate Authority Ty	Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 Intermediate CA Request	-	
	Create			

3. Select the default CA certificate, and click **Download** to export the CA certificate of the key management server.

1.5.3 Creating a Local User

This section describes the precautions for creating a local user on a key management server. This user is used by the key management server to authenticate a storage system using the Key Management Interoperability Protocol (KMIP).

Precautions

To ensure that the key management server can identify the storage system successfully, the local user name of the key management server must be set to **Storage**, which is the same as the **OU** value in the signed certificate of the storage system.

You can query the **OU** value as follows:

- 1. Double-click the certificate.
- 2. Click the **Detail** tab, and select **User**. You can view the **OU** value in the lower pane.

CN = WH RSA CA	
OV = Storage	
0 = Huawei	
L = ChengDu	
S = SiChuan	
C = CN	
1	

Context

Create at least one local user.

Procedure

- 1. Log in as the **admin** user to the key management server's web interface.
- 2. Choose **Security > Users & Groups > Local Users & Groups > Local Users**.

The User & Group Configuration page is displayed, as shown in Figure 1.



Home • Security •	Device					Help 🔹 Log Out
Keys & KMIP Objects Keys KMIP Objects	Security / Local Users	<u>s & Groups</u> / Local U Group Co	onfiguration			vESKM Logged in as admin
Authorization Policies	Local Users					Help 📀
Users & Groups Local Users & Groups	Filtered by Items per page: 10	where value Submit	contains v	Set Filter		
Local Users	🔺 Username	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
Local Groups LDAP	Add Delete P	roperties				
Certificates & CAs						
Certificates						
Inusted CA Lists Local CAs						
Known CAs						
Advanced Security						
High Security						
SSL Options						
SSH Options						
FIPS Status Server						

3. In the Local User area, click Add.

Figure 2 shows the page that is displayed.

Figure 2 Local user information setting page

Marge Coged in as at Marge Coged in as at Coged in as at Coged in as at Contraction Policies Contraction Policies Contraction Policies Password: Contraction Policies Password: Contraction Policies Password: Contraction Policies Contraction Policies Contraction Policies Password: Contraction Password: Contraction Policies Contraction Password: Contraction Password: Status Beaution Contraction Password: Mapnon-existent Object Group: Endel Khill: Mapnon-existent Object Group: Endel Khill: Status Beaver Khill? Client Certificate: File? Contraction Password: File? <t< th=""><th>Kevs & KMIP Objects</th><th>Security / Local Users & Groups / Local Users</th><th></th><th>VESR</th></t<>	Kevs & KMIP Objects	Security / Local Users & Groups / Local Users		VESR
 KMIP Objekti Authorization Policies Create Local User Create Local	Keys			Logged in as adm
• Atthriztion Policies Vector & Groupp Local Users & Groups Local Groups Local Groups Local Groups Local Groups Local Groups Confirm Password: Locan Confirm Password: Confirm Password: Confirm Password: Confirm Password: Confirm Password: Confirm Password: Grand Confirm Password: Grand Confirm Password: Grand Confirm Password: Grand Confirm Password: Confirm Password: Grand Confirm Password: Grand Confirm	 KMIP Objects 	Create Local User		
Users & Groups Username: Local Users & Groups Confirm Password: Confirm Password: Granded Scales Granded Scales Map non-existent Object Group: KMIP User Group:	Authorization Policies	Create Local User		Help
Local Users & Groups I. Local Users & Charler & Confirm Password: Local Confirm Password: User Administration Permission: Certificates & CAS Certificates & CAS Confirm Password: Certificates & CAS Confirm Password: Certificates & CAS Confirm Password: Certificates & CAS Certificates & CAS KMIP Object Group: KMIP Object Group: KMIP Client Certificate: FIPS Status Server KMIP Client Dertificate: Certificates Server	Jsers & Groups			
• Local Groups > Local CAs • Certificates • Cortificates • Cortificates • Local CAs • Korom CAs • Map non-existent Object Group: • KMIP Object Group: • Gefault user group ▼ • KMIP Object Group: • Gefault user group ▼ • KMIP Object Group: • Bis Options • FIPS Status Server	 Local Users & Groups 	Username:		-
Lacal Groups Confirm Password:	Local Users	Password:		
▶ LDAP License Type: Uncategorised ▼ • Certificates Change Password Permission: □ • Certificates Enable KMIP Ø • Trusted CA Lists Enable KMIP Ø • Local CAs KMIP User Group: @ default user group ▼ • Known CAs KMIP Object Group: @ default user group ▼ • High Security SSL Options • SSH Options FIPS Status Server	Local Groups	Confirm Password:]
Uer Administration Permission: Centrificates & CAS Centrificates & CAS Centrificates Trusted CA Lists KMIP Object Group to x-Object Group: KMIP Object Group: Centrificates KMIP Client Certificate: KMIP Client Certificate: KMIP Client Certificate: KMIP Client Certificate: Create Create Centrificates Centrif	LDAP	License Type:	Uncategorised V	
Certificates • Certificates • Tursted CALists • Local CAS • Known CAS KMIP Client Certificate: • FIPS Status Server • Create Cencel		User Administration Permission:		
Certificates Enable KMIP: © Trusted CA Lists Map non-existent Object Group: □ Local CAs KMIP Object Group: □ Known CAs KMIP Object Group: □ Warneed Security KMIP Object Group: □ High Security KMIP Object Group: □ SSL Options KMIP Client Certificate: FIPS Status Server KMIP Client Certificate:	Certificates & CAs	Change Password Permission:		-
 Tusted CALisis Local CAS Known CAS KMIP User Group: default user group ▼ KMIP Client Certificate: KMIP Client Certificate: FIPS Status Server 	 Certificates 	Enable KMIP:		-
 Local CAs Known CAs KMIP User Group: default user group ▼ KMIP Client Certificate: KMIP Client Certificate: FIPS Status Server 	Trusted CA Lists	Map non-existent Object Group to x-Object Group:		-
 Known CAs KMIP Object Group: default object group ▼ KMIP Client Certificate: SH Options FIPS Status Server Create Cencel 	Local CAs	KMIP User Group:	default user group 🗸	
Advanced Security	 Known CAs 	KMIP Object Group:	default object group 🗸	
High Security SSL Options SSH Options FIPS Status Server	Advanced Security	KMIP Client Certificate		
SSL Options SSL Options FIPS Status Server Create Cancel	High Security	Tum Onen Germoure.		
SSH Options FIPS Status Server	SSL Ontions			
FIPS Status Server Create Cancel	SSH Options			
Create Cancel	EIRC Status Conver			
Create	FIFS Status Server			
Oreate Cencel				
Dreste Cancel				
Create Cancel				
Create				
Create				
Create Cencel				
Create Cancel				
Create Cancel				
Create Cancel			4	
		Create Cancel		

NOTICE

Enter the signed.crt certificate content downloaded in 5 in the KMIP Client Certificate area.

Table 1 User parameters

Parameter	Description	Setting
Username	Name of the new user. Set the value to Storage .	[Example] Storage
Password	Password of the new user.	[Example] admin@123
Confirm Password	Enter the password again.	[Example] admin@123
License Type	License type of the key management server. To connect to a storage device, select Storage .	[Example] Storage
User Administration Permission	Permission to create, modify, and delete a user or user group.	[Example] Not selected
Change Password Permission	Permission to modify a user's own password.	[Example] Not selected
Enable KMIP	The KMIP protocol that should be selected for storage system authentication.	[Example] Selected

D NOTE

For **Map non-existent Object Group to x-Object Group**, **KMIP User Group**, and **KMIP Object Group**, use the default values.

5. Click Create.

The new user is displayed in the user list, as shown in Figure 3.



Home • Security •	Device					Help 🔸 Log Out
Keys & KMIP Objects Keys KMIP Objects	Security / Local User	<u>s & Groups</u> / Local U Group Co	onfiguration			vESKM Logged in as admin
Authorization Policies	Local Users					Help 🕜
Users & Groups Local Users & Groups	Filtered by Items per page: 10	where valu Submit	e contains 🗸	Set Filter		
Local Users	LUSername	KMIP-Enabled	User Administration Permission	Change Password Permission	License Type	Last Access Time
Local Groups LDAP	Storage			1 - 1 of 1	Storage	2021-03-02 20:02:06
Certificates & CAs	Add Delete P	Topernes				
Certificates Trusted CA Lists						
+ Local CAs						
Known CAs						
Advanced Security						
High Security Sci. Options						
SSH Options						
FIPS Status Server						

1.5.4 Importing and Activating the Certificate on the Storage System

This section describes how to import and activate the certificate on the storage system.

Procedure

- 1. Log in to DeviceManager.
- 2. Choose Settings > Certificates.
- 3. Import and activate the certificate.
 - a. On the Certificate Management page, choose KMC certificate, and click Import Certificate.

D NOTE

You can also click **KMC certificate**. On the **Certificate Details** page that is displayed, click **Operation > Import Certificate**.

b. Import the signed certificate and CA certificate. <u>Table 1</u> describes the parameters.

Table 1 Parameters for importing the certificate

Parameter	Description	Value
Certificate File	Certificate file that has been exported and signed	[Example] signed.crt
CA Certificate File	Certificate file of a server	[Example] ESKMCA.crt
Private Key File	Private key file of a device	[Example] None

c. Click OK.

The Warning dialog box is displayed.

d. Carefully read the content in the dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

The **Success** dialog box is displayed.

e. Click OK.

1.5.5 Configuring the External Key Service on the Storage System

You must configure the key management servers on the storage system to establish the connection between them.

Context

A storage system needs two key management servers.

Procedure

- 1. Log in to DeviceManager.
- 2. Choose **Settings** > **Key Service**. In the function pane on the right, click **Modify**.

Then select **Enable the external key service**.

3. Specify the key management server parameters listed in <u>Table 1</u>.

D NOTE

A storage system can connect to a maximum of two key management servers in a cluster. The following example adds one key management server to the storage system.

Table 1 Key server parameters

Parameter	Description	Value
Server	Type of the key server.	[Example] SafeNet KMIP
Type	Thales KMIP refers to the Thales keyAuthority key server.	
	SafeNet KMIP refers to the Thales CipherTrust Manager key server and KeySecure key server.	
	General KMIP is compatible with SafeNet KMIP and Utimaco KMIP.	
	HashiCorp Vault KMIP refers to the HashiCorp Vault key server.	
Address	Domain name or service IP address of the key server.	[Example]
		192.168.141.128
Port	Port number of the key server IP address.	[Value range]
		1 to 65535
		[Default Value]
		9443

4. Import the signed certificate and CA certificate. <u>Table 2</u> describes the parameters.

Table 2 Parameters for importing the certificate

Parameter	Description	Value
Certificate File	Certificate file that has been exported and signed.	[Example] signed.crt
CA Certificate File	Certificate file of a server.	[Example] hsm.mgmt_ca.crt
Private Key File	Private key file of a device.	[Example] None

5. Click Save.

The Execution Result dialog box is displayed.

6. Repeat $\underline{3}$ to add the other key management server in the cluster.

Follow-up Procedure

After the storage system has connected to the key management servers, wait for 2 to 3 minutes before performing follow-up procedures.

1.6 Creating a Self-encrypting Storage Pool (Using SEDs)

After a self-encrypting storage pool is created on the storage system, an encryption key is automatically generated.

Prerequisites

SEDs have been configured on the storage system. The AutoLock status of the SEDs is OFF.

To query the **AutoLock** status of the SEDs, you can log in to the CLI of the storage system and run the **show disk general** command.

admin:/>show disk general								
ID Health Stat	us Running Sta	tus Type	Capacity R	Role D	oisk Domai	n ID Sp	eed(RP	PM) Health Mark Bar Code Item
AutoLock State Key Expiration Time								
DAE000.0 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FB000131 02350LGX
OFF								
DAE000.1 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FB000124 02350LGX
OFF								
DAE000.2 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FB000238 02350LGX
OFF								
DAE000.3 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FA000228 02350LGX
OFF								
DAE000.4 Norma	l Online	SSD-SED	371.965GB	Free D	isk			2102350LGX10FA000227 02350LGX
OFF								
DAE000.5 Norma	l Online	SSD-SED	371.965GB	Free D	isk			2102350LGX10FA000187 02350LGX
OFF								
DAE100.0 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FA000159 02350LGX
OFF								
DAE100.1 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FA000161 02350LGX
OFF								
DAE100.2 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10G3000505 02350LGX
OFF								
DAE100.3 Norma	l Online	SSD-SED	366.965GB	Free D	isk			2102350LGX10FA000182 02350LGX
OFF								
DAE100.4 Norma	l Online	SSD-SED	371.965GB	Free D	isk			2102350LGX10G3000511 02350LGX
OFF								

If AutoLock State is OFF, disk encryption is disabled.

Procedure

 Log in to DeviceManager and create a storage pool. The Create Storage Pool page is displayed.

Figure 1 Creating a storage pool

Create Storage P	ool 🛛		Advanced
* Name	StoragePool002		
* Redundancy Policy	Disk redundancy	•	
* Controller Enclosure Storage Pool Capacity	CTE0		
Capacity per Disk Type	Available Disks	Selectable Disks per Controller Enclosure ③	Required Disks ⑦
Total: 0 < 1 >		No data.	
		OK Cancel	

Use either of the following methods to go to the Create Storage Pool page:

- When you log in to the storage system for the first time, you can create a storage pool in **Custom** mode in the initial configuration wizard. For details, see "Initially Configuring a Storage Device" in the initialization guide specific to your product model.
- On the menu bar, choose **System** > **Storage Pools** and then click **Create**.
- 2. Create a self-encrypting storage pool and automatically generate encryption keys on the storage system.
 - a. Select **Advanced** and enable **Data Encryption**. Disk encryption is enabled for all SEDs in the storage pool.

Create Stor	age Pool @	Z Advanced
* Name	StoragePool002	
Description	0 to 255 characters	
Data Encryptior	Confirm your key service configuration.	

D NOTE

0 0

1.1.

D · D

After a storage pool has been created, data encryption cannot be enabled or disabled for the storage pool.

b. Set other parameters for the storage pool.

For the parameter description, see section "Creating a Storage Pool" in the *Basic Storage Service Configuration Guide for Block* or *Basic Storage Service Configuration Guide for File* of the specific product model.

c. Click OK.

Confirm your operation as prompted.

Follow-up Procedure

After creating the self-encrypting storage pool, you can create LUNs or file systems to allocate the storage space to application servers. For details, see *Basic Storage Service Configuration Guide for Block* or *Basic Storage Service Configuration Guide for File* of the corresponding product model.



You can log in to Huawei's technical support website (<u>https://support.huawei.com/enterprise/</u>) and enter the product model + document name in the search box to search for, browse, and download the desired documents.

1.7 Creating a Self-encrypting Storage Pool (Using the Data Encryption Function, Applicable to 6.1.5 and Later Versions)

This section describes how to create a self-encrypting storage pool by using the data encryption function.

Checking the License

Creating a Self-encrypting Storage Pool

1.7.1 Checking the License

Prerequisites

The HyperEncryption license has been imported and activated.

Context

On DeviceManager, the data encryption feature name is **HyperEncryption**.

Procedure

- 1. Log in to DeviceManager.
- 2. Choose Settings > License Management.
- 3. In the middle function pane, check that the activated license contains HyperEncryption.

1.7.2 Creating a Self-encrypting Storage Pool

This section describes how to create a self-encrypting storage pool for non-SEDs by using the data encryption function.

Procedure

1. Log in to DeviceManager and create a storage pool.

The **Create Storage Pool** page is displayed.

Figure 1 Creating Create Storage P	a storage pool ool ©			Advanced
* Name	StoragePool002			
* Redundancy Policy	Disk redundancy	•		
* Controller Enclosure Storage Pool Capacity	СТЕО			
Capacity per Disk Type	Available Disks	Selectable Disks per	Controller Enclosure ③	Required Disks ⑦
Total: 0 < 1 >		No data.		
		OK Cancel		

D NOTE

Use either of the following methods to go to the Create Storage Pool page:

- When you log in to the storage system for the first time, you can create a storage pool in **Custom** mode in the initial configuration wizard. For details, see "Initially Configuring a Storage Device" in the initialization guide specific to your product model.
- On the menu bar, choose System > Storage Pools and then click Create.
- 2. Create a self-encrypting storage pool.
 - a. Select **Advanced** and enable **Data Encryption**. Disk encryption is enabled for all disks in the storage pool.

Figure 2 Crea Create Stora	ting a self-encrypting storage pool ge Pool @	Advanced
* Name	StoragePool002	
Description	0 to 255 characters	
Data Encryption	Confirm your key service configuration.	

- b. Set other parameters to create the self-encrypting storage pool. For the parameter description, see section "Creating a Storage Pool" in the *Basic Storage Service Configuration Guide for Block* or *Basic Storage Service Configuration Guide for File* of the specific product model.
- c. Click **OK** and confirm your operation as prompted.



After the self-encrypting storage pool has been created, you cannot change the enabling status of **Data Encryption** for the storage pool.

3. View the encryption key on the key management server.

Follow-up Procedure

After creating the self-encrypting storage pool, you can create LUNs or file systems to allocate the storage space to application servers. For details, see *Basic Storage Service Configuration Guide for Block* or *Basic Storage Service Configuration Guide for File* of the corresponding product model.

D NOTE

You can log in to Huawei's technical support website (<u>https://support.huawei.com/enterprise/</u>) and enter the product model + document name in the search box to search for, browse, and download the desired documents.