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.

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.

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

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.

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. Figure 1 shows the typical networking.

Figure 1 Typical networking of key management servers

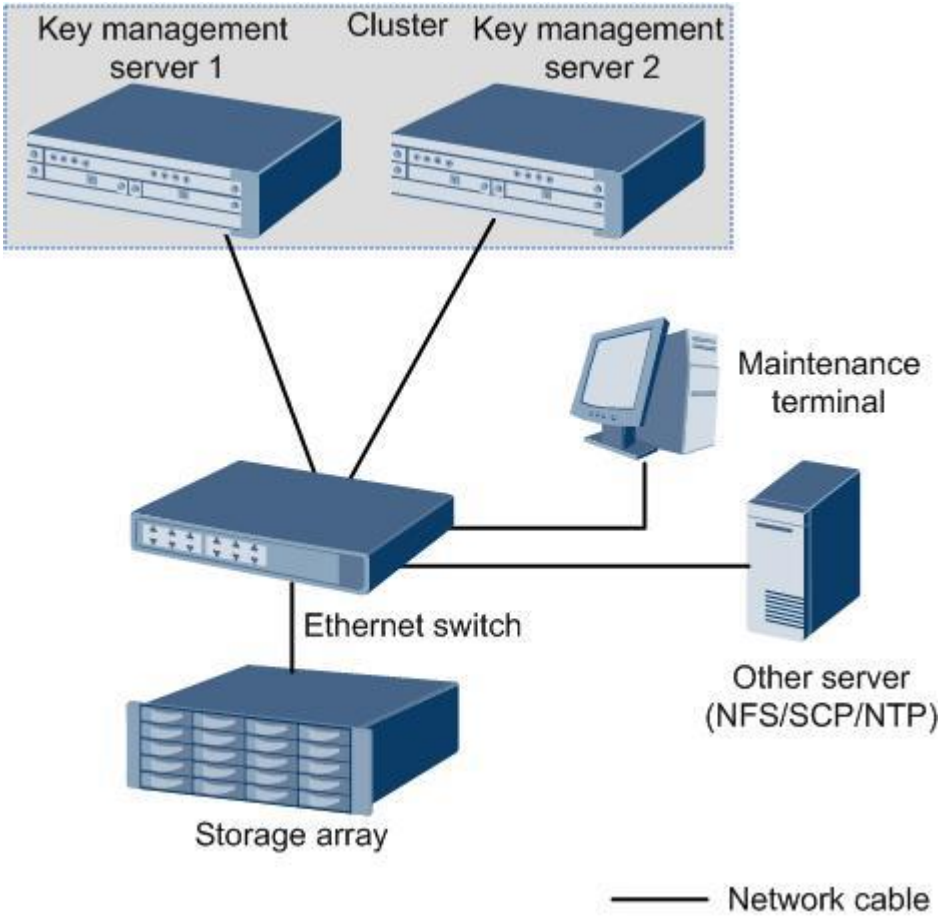
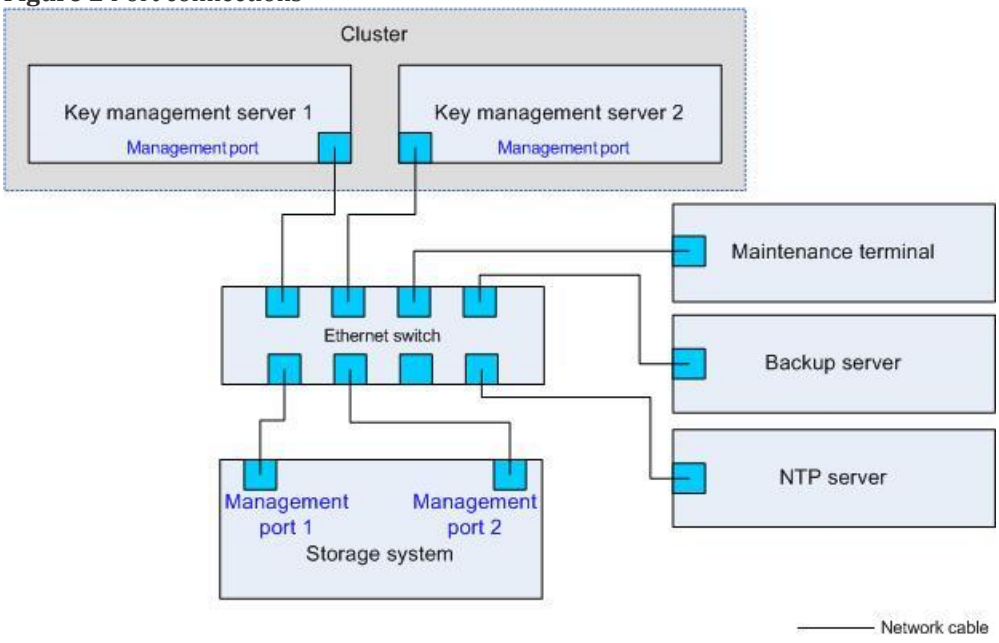


Figure 2 shows port connections between different components.

Figure 2 Port connections



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

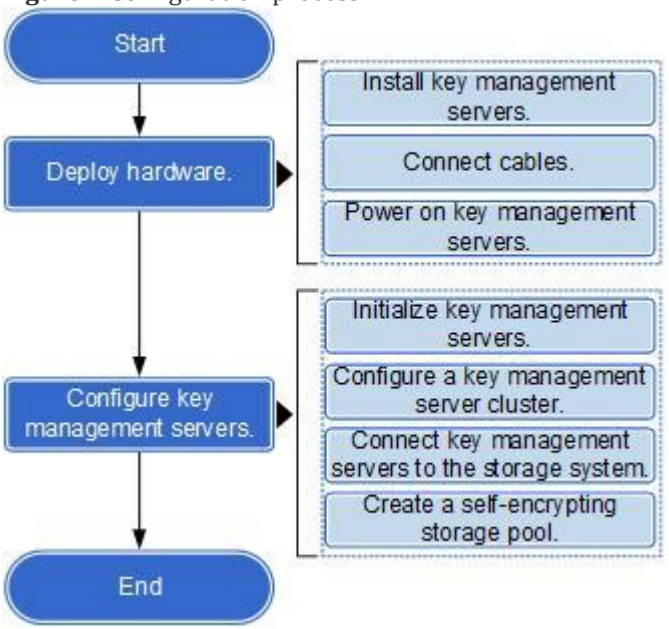
- Backup server's network port -> key management servers' LAN1

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)

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 3 to 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**.

   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**.

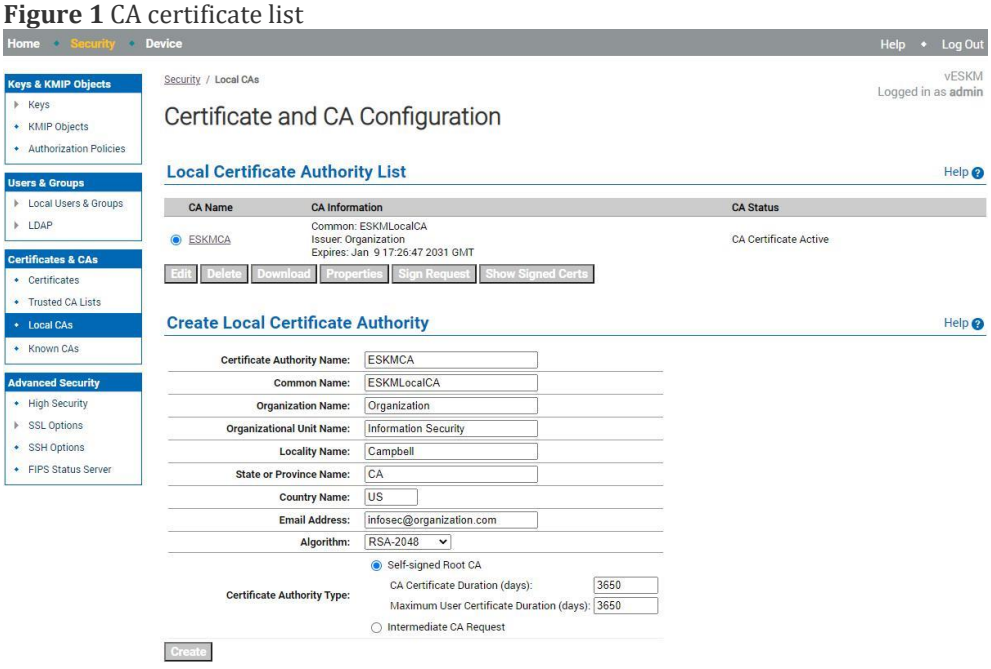
1.5.2 Signing the Certificate on a Key Management Server and Exporting the Certificate

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

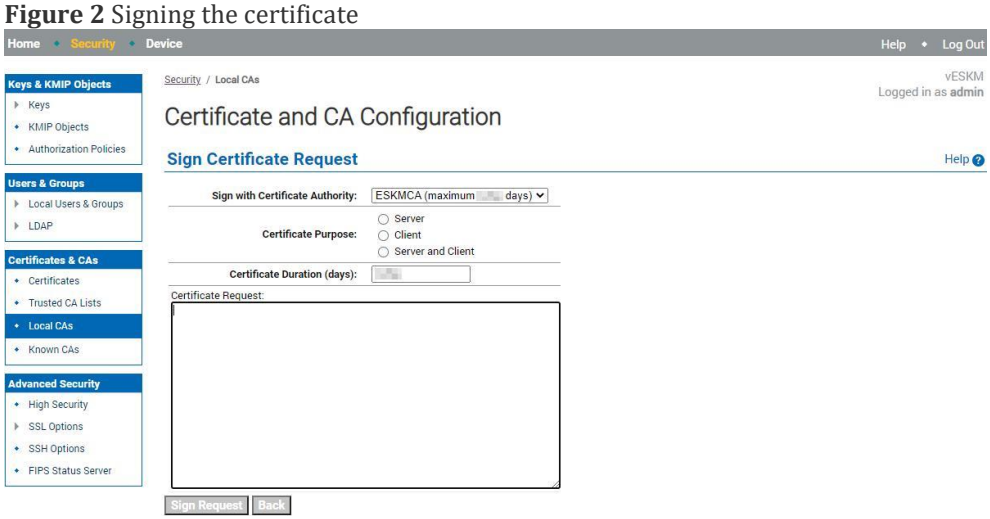
1. Log in to the key management server's web interface as an administrator.
2. Choose **Security** > **Certificates & CAs > Local CAs**.
   The **Certificate and CA Configuration** interface is displayed, as shown in Figure 1.

Figure 1 CA certificate list



3. Select the default CA certificate and click **Sign Request**.
   The **Sign Certificate Request** interface is displayed, as shown in Figure 2.

Figure 2 Signing the certificate



4. Set certificate request parameters.

   a. Set **Sign with Certificate Authority** to **ESKMCA (maximum xxxx days)** (default value).

   b. Set **Certificate Purpose** to **Client**.

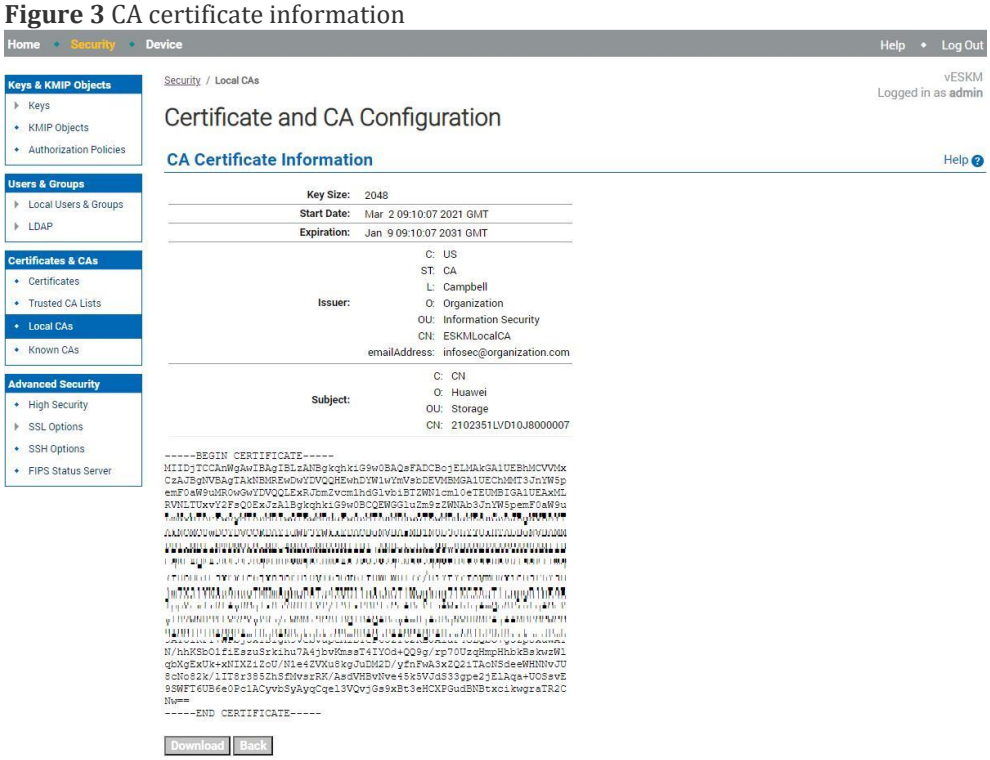
   c. Set **Certificate Duration (days)** to the validity period of the certificate. The value of this parameter must not be greater than **xxx** in **ESKMCA (maximum xxxx days)**.

   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.

Figure 3 CA certificate information



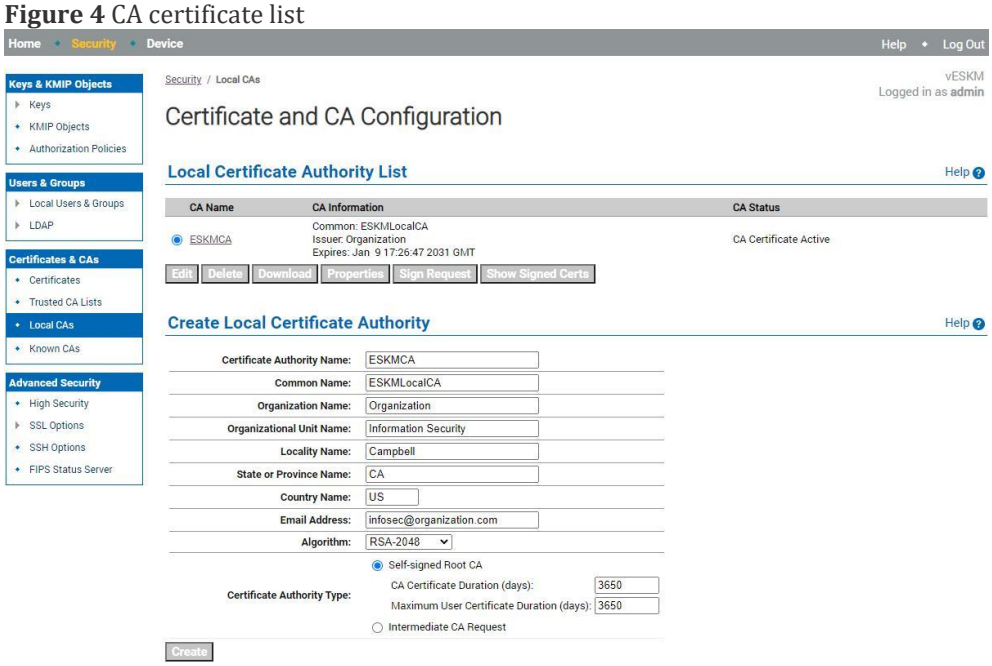
5. Click **Download** to export the signed certificate.

   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



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.

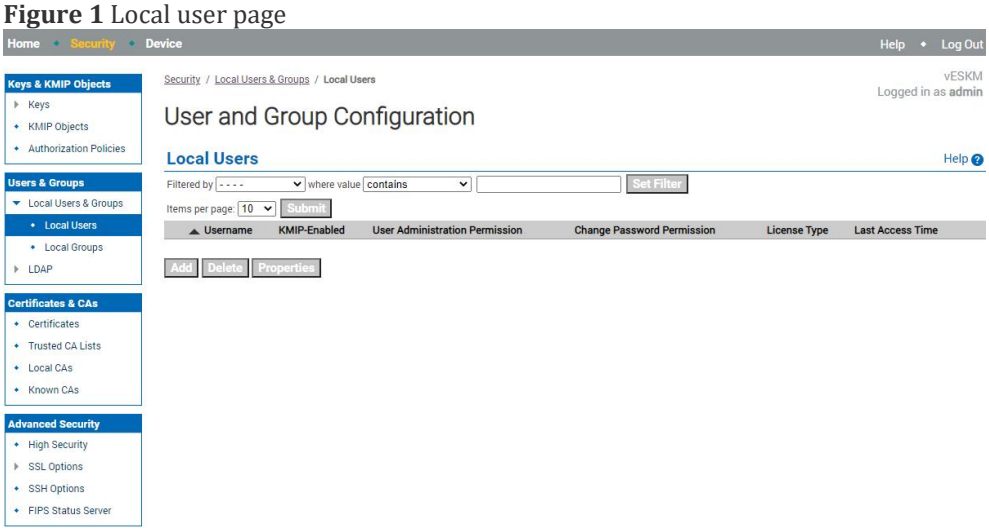
Context

Create at least one local user.

Procedure

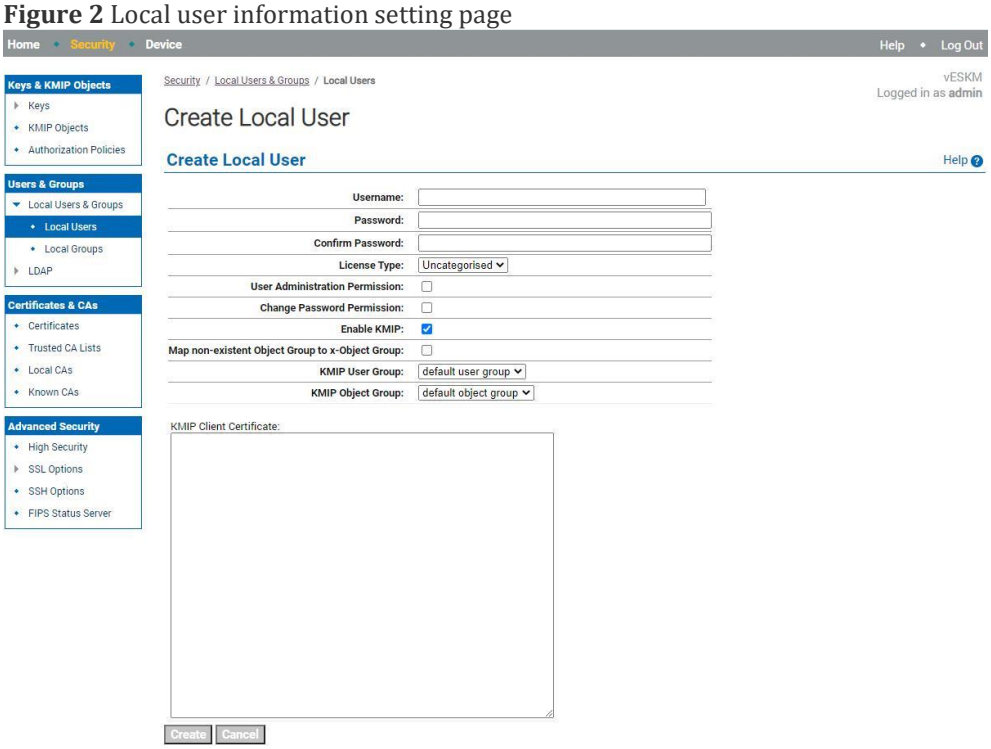
1. Log in as the **admin** user to the key management server's web interface.
2. Choose **Security** > **Users & Groups** > **Local Users & Groups** > **Local Users**.
   The **User & Group Configuration** page is displayed, as shown in Figure 1.

Figure 1 Local user page



3. In the **Local User** area, click **Add**.
   Figure 2 shows the page that is displayed.

Figure 2 Local user information setting page



4. Set user information.

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

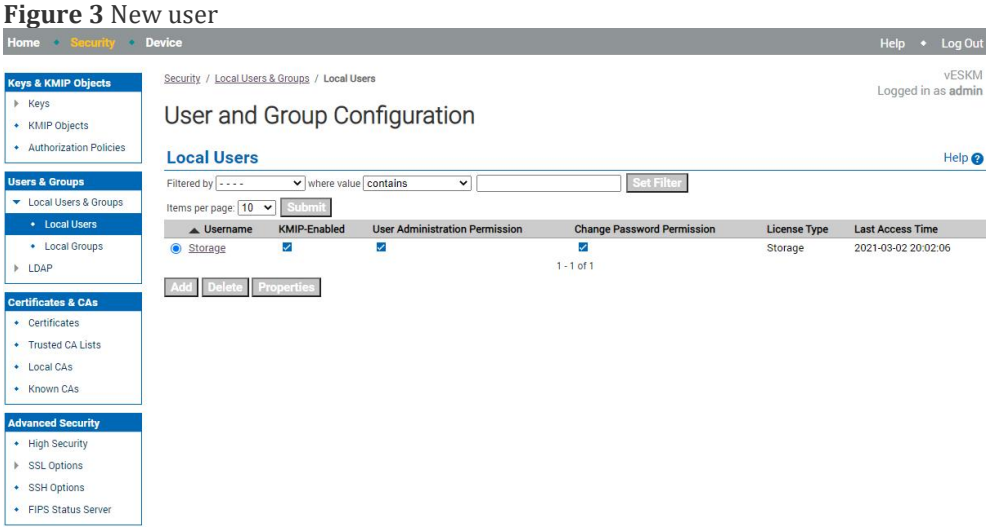
NOTE

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.

Figure 3 New user



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**.

      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. Table 1 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 Table 1.

   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	Type of the key server. **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.	[Example] SafeNet KMIP
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. Table 2 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 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 Status  Running Status  Type     Capacity   Role      Disk Domain ID  Speed(RPM)  Health Mark  Bar Code           Item
AutoLock State  Key Expiration Time
 ------ -------------- --------------- -------- ---------- ---------- --------------- ----------- ------------ ---------------------- --------- --------------- -----------------
---
DAE000.0  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FB000131  02350LGX
OFF  --
DAE000.1  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FB000124  02350LGX
OFF  --
DAE000.2  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FB000238  02350LGX
OFF  --
DAE000.3  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FA000228  02350LGX
OFF  --
DAE000.4  Normal       Online        SSD-SED   371.965GB  Free Disk  --          --        --         2102350LGX10FA000227  02350LGX
OFF  --
DAE000.5  Normal       Online        SSD-SED   371.965GB  Free Disk  --          --        --         2102350LGX10FA000187  02350LGX
OFF  --
DAE100.0  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FA000159  02350LGX
OFF  --
DAE100.1  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FA000161  02350LGX
OFF  --
DAE100.2  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10G3000505  02350LGX
OFF  --
DAE100.3  Normal       Online        SSD-SED   366.965GB  Free Disk  --          --        --         2102350LGX10FA000182  02350LGX
OFF  --
DAE100.4  Normal       Online        SSD-SED   371.965GB  Free Disk  --          --        --         2102350LGX10G3000511  02350LGX
OFF  --
```

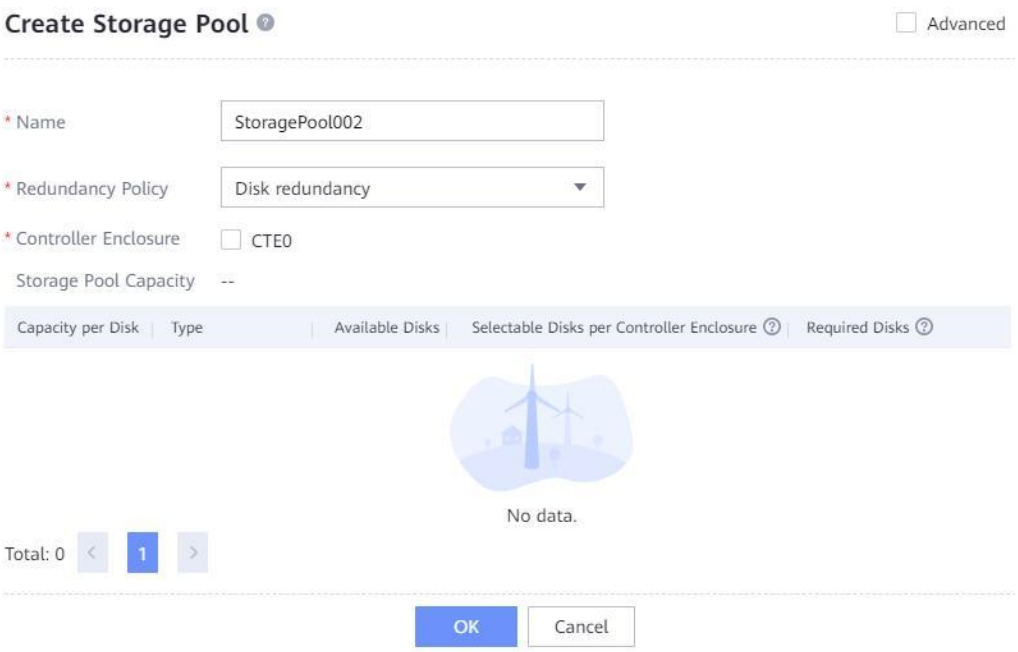
If **AutoLock State** is **OFF**, disk encryption is disabled.

Procedure

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

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

   Figure 1 Creating a storage pool



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 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.

   Figure 2 Enabling **Data Encryption**

   NOTE

   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.

NOTE

You can log in to Huawei's technical support website (https://support.huawei.com/enterprise/) 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.

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

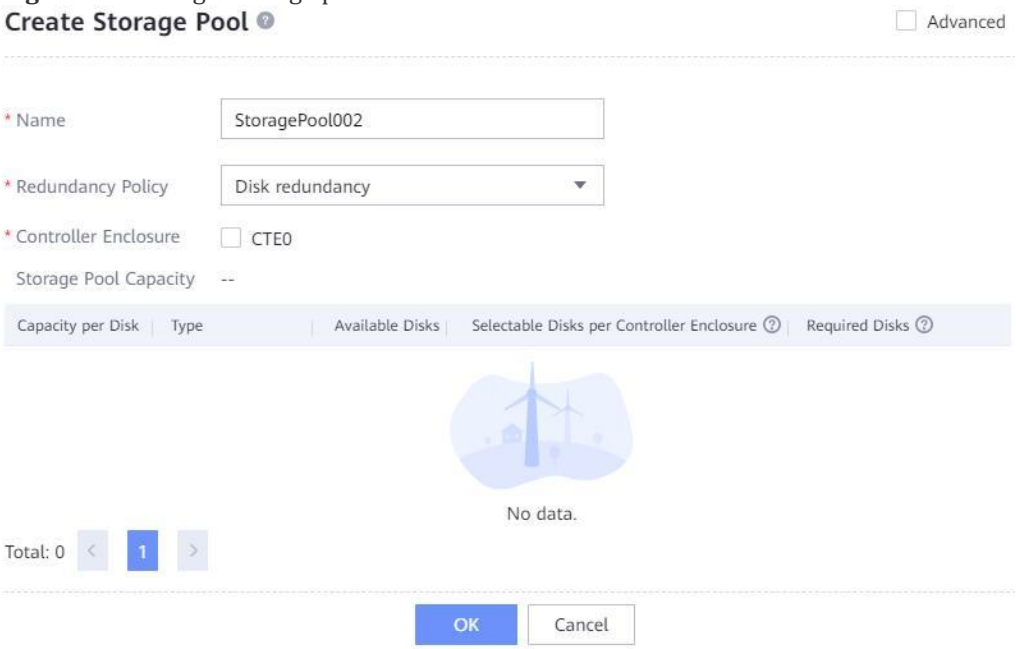
This section describes how to create a self-encrypting storage pool for non-SEDs by using the data encryption function.

Procedure

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

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

Figure 1 Creating a storage pool



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 Creating a self-encrypting storage pool

   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.

   NOTE

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.

NOTE

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