NetApp

Configure key management servers

StorageGRID

NetApp
March 03, 2022

Table of Contents

Configure key management servers

Configure key management servers: Overview

You can configure one or more external key management servers (KMS) to protect the data on specially configured appliance nodes.

What is a key management server (KMS)?

A key management server (KMS) is an external, third-party system that provides encryption keys to StorageGRID appliance nodes at the associated StorageGRID site using the Key Management Interoperability Protocol (KMIP).

You can use one or more key management servers to manage the node encryption keys for any StorageGRID appliance nodes that have the **Node Encryption** setting enabled during installation. Using key management servers with these appliance nodes lets you protect your data even if an appliance is removed from the data center. After the appliance volumes are encrypted, you cannot access any data on the appliance unless the node can communicate with the KMS.

> ⓘ StorageGRID does not create or manage the external keys used to encrypt and decrypt appliance nodes. If you plan to use an external key management server to protect StorageGRID data, you must understand how to set up that server, and you must understand how to manage the encryption keys. Performing key management tasks is beyond the scope of these instructions. If you need help, see the documentation for your key management server or contact technical support.

Review StorageGRID encryption methods

StorageGRID provides a number of options for encrypting data. You should review the available methods to determine which methods meet your data-protection requirements.

The table provides a high-level summary of the encryption methods available in StorageGRID.

Encryption option	How it works	Applies to
Key management server (KMS) in Grid Manager	You configure a key management server for the StorageGRID site (**CONFIGURATION** > **Security** > **Key management server**) and enable node encryption for the appliance. Then, an appliance node connects to the KMS to request a key encryption key (KEK). This key encrypts and decrypts the data encryption key (DEK) on each volume.	Appliance nodes that have **Node Encryption** enabled during installation. All data on the appliance is protected against physical loss or removal from the data center. Can be used with some StorageGRID storage and services appliances.

Encryption option	How it works	Applies to
Drive security in SANtricity System Manager	If the Drive Security feature is enabled for a storage appliance, you can use SANtricity System Manager to create and manage the security key. The key is required to access the data on the secured drives.	Storage appliances that have Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. All data on the secured drives is protected against physical loss or removal from the data center. Cannot be used with some storage appliances or with any service appliances. • SG6000 storage appliances • SG5700 storage appliances • SG5600 storage appliances
Stored Object Encryption grid option	The **Stored Object Encryption** option can be enabled in the Grid Manager (**CONFIGURATION** > **System** > **Grid options**). When enabled, any new objects that are not encrypted at the bucket level or at the object level are encrypted during ingest.	Newly ingested S3 and Swift object data. Existing stored objects are not encrypted. Object metadata and other sensitive data are not encrypted. • Configure stored object encryption
S3 bucket encryption	You issue a PUT Bucket encryption request to enable encryption for the bucket. Any new objects that are not encrypted at the object level are encrypted during ingest.	Newly ingested S3 object data only. Encryption must be specified for the bucket. Existing bucket objects are not encrypted. Object metadata and other sensitive data are not encrypted. • Use S3
S3 object server-side encryption (SSE)	You issue an S3 request to store an object and include the `x-amz-server-side-encryption` request header.	Newly ingested S3 object data only. Encryption must be specified for the object. Object metadata and other sensitive data are not encrypted. StorageGRID manages the keys. • Use S3

Encryption option	How it works	Applies to
S3 object server-side encryption with customer-provided keys (SSE-C)	You issue an S3 request to store an object and include three request headers. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Newly ingested S3 object data only. Encryption must be specified for the object. Object metadata and other sensitive data are not encrypted. Keys are managed outside of StorageGRID. • Use S3
External volume or datastore encryption	You use an encryption method outside of StorageGRID to encrypt an entire volume or datastore, if your deployment platform supports it.	All object data, metadata, and system configuration data, assuming every volume or datastore is encrypted. An external encryption method provides tighter control over encryption algorithms and keys. Can be combined with the other methods listed.
Object encryption outside of StorageGRID	You use an encryption method outside of StorageGRID to encrypt object data and metadata before they are ingested into StorageGRID.	Object data and metadata only (system configuration data is not encrypted). An external encryption method provides tighter control over encryption algorithms and keys. Can be combined with the other methods listed. • Amazon Simple Storage Service - Developer Guide: Protecting data using client-side encryption

Use multiple encryption methods

Depending on your requirements, you can use more than one encryption method at a time. For example:

- You can use a KMS to protect appliance nodes and also use the drive security feature in SANtricity System Manager to "double encrypt" data on the self-encrypting drives in the same appliances.
- You can use a KMS to secure data on appliance nodes and also use the Stored Object Encryption grid option to encrypt all objects when they are ingested.

If only a small portion of your objects require encryption, consider controlling encryption at the bucket or

individual object level instead. Enabling multiple levels of encryption has an additional performance cost.

Overview of KMS and appliance configuration

Before you can use a key management server (KMS) to secure StorageGRID data on appliance nodes, you must complete two configuration tasks: setting up one or more KMS servers and enabling node encryption for the appliance nodes. When these two configuration tasks are complete, the key management process occurs automatically.

The flowchart shows the high-level steps for using a KMS to secure StorageGRID data on appliance nodes.
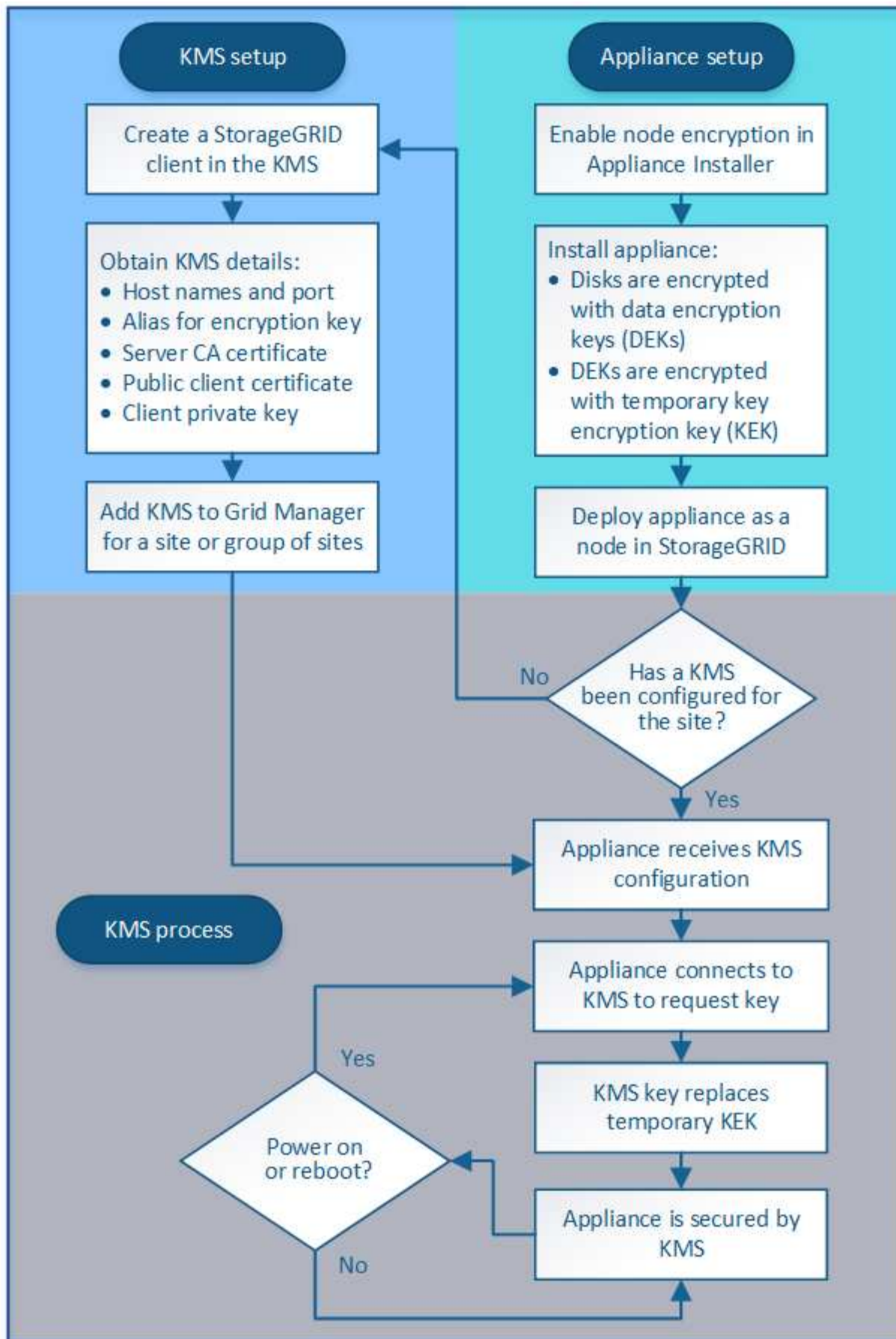
The flowchart shows KMS setup and appliance setup occurring in parallel; however, you can set up the key

management servers before or after you enable node encryption for new appliance nodes, based on your requirements.

Set up the key management server (KMS)

Setting up a key management server includes the following high-level steps.

Step	Refer to
Access the KMS software and add a client for StorageGRID to each KMS or KMS cluster.	Configure StorageGRID as a client in the KMS
Obtain the required information for the StorageGRID client on the KMS.	Configure StorageGRID as a client in the KMS
Add the KMS to the Grid Manager, assign it to a single site or to a default group of sites, upload the required certificates, and save the KMS configuration.	Add a key management server (KMS)

Set up the appliance

Setting up an appliance node for KMS use includes the following high-level steps.

1. During the hardware configuration stage of appliance installation, use the StorageGRID Appliance Installer to enable the **Node Encryption** setting for the appliance.

   (i) You cannot enable the **Node Encryption** setting after an appliance is added to the grid, and you cannot use external key management for appliances that do not have node encryption enabled.

2. Run the StorageGRID Appliance Installer. During installation, a random data encryption key (DEK) is assigned to each appliance volume, as follows:

   ◦ The DEKs are used to encrypt the data on each volume. These keys are generated using Linux Unified Key Setup (LUKS) disk encryption in the appliance OS and cannot be changed.

   ◦ Each individual DEK is encrypted by a master key encryption key (KEK). The initial KEK is a temporary key that encrypts the DEKs until the appliance can connect to the KMS.

3. Add the appliance node to StorageGRID.

For details, refer to the following:

- SG100 and SG1000 services appliances
- SG6000 storage appliances
- SG5700 storage appliances
- SG5600 storage appliances

Key management encryption process (occurs automatically)

Key management encryption includes the following high-level steps that are performed automatically.

1. When you install an appliance that has node encryption enabled into the grid, StorageGRID determines if a KMS configuration exists for the site that contains the new node.

   ◦ If a KMS has already been configured for the site, the appliance receives the KMS configuration.

   ◦ If a KMS has not yet been configured for the site, data on the appliance continues to be encrypted by the temporary KEK until you configure a KMS for the site and the appliance receives the KMS configuration.

2. The appliance uses the KMS configuration to connect to the KMS and request an encryption key.

3. The KMS sends an encryption key to the appliance. The new key from the KMS replaces the temporary KEK and is now used to encrypt and decrypt the DEKs for the appliance volumes.

   > ⓘ Any data that exists before the encrypted appliance node connects to the configured KMS is encrypted with a temporary key. However, the appliance volumes should not be considered protected from removal from the data center until the temporary key is replaced by the KMS encryption key.

4. If the appliance is powered on or rebooted, it reconnects to the KMS to request the key. The key, which is saved in volatile memory, cannot survive a loss of power or a reboot.

Considerations and requirements for using a key management server

Before configuring an external key management server (KMS), you must understand the considerations and requirements.

What are the KMIP requirements?

StorageGRID supports KMIP version 1.4.

[Key Management Interoperability Protocol Specification Version 1.4](#)

Communications between the appliance nodes and the configured KMS use secure TLS connections. StorageGRID supports the following TLS v1.2 ciphers for KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

You must ensure that each appliance node that uses node encryption has network access to the KMS or KMS cluster you configured for the site.

The network firewall settings must allow each appliance node to communicate through the port used for Key Management Interoperability Protocol (KMIP) communications. The default KMIP port is 5696.

Which appliances are supported?

You can use a key management server (KMS) to manage encryption keys for any StorageGRID appliance in your grid that has the **Node Encryption** setting enabled. This setting can only be enabled during the hardware configuration stage of appliance installation using the StorageGRID Appliance Installer.

(i) You cannot enable node encryption after an appliance is added to the grid, and you cannot use external key management for appliances that do not have node encryption enabled.

You can use the configured KMS for the following StorageGRID appliances and appliance nodes:

Appliance	Node type
SG1000 services appliance	Admin Node or Gateway Node
SG100 services appliance	Admin Node or Gateway Node
SG6000 storage appliance	Storage Node
SG5700 storage appliance	Storage Node
SG5600 storage appliance	Storage Node

You cannot use the configured KMS for software-based (non-appliance) nodes, including the following:

- Nodes deployed as virtual machines (VMs)
- Nodes deployed within container engines on Linux hosts

Nodes deployed on these other platforms can use encryption outside of StorageGRID at the datastore or disk level.

When should I configure key management servers?

For a new installation, you should typically set up one or more key management servers in the Grid Manager before creating tenants. This order ensures that the nodes are protected before any object data is stored on them.

You can configure the key management servers in the Grid Manager before or after you install the appliance nodes.

How many key management servers do I need?

You can configure one or more external key management servers to provide encryption keys to the appliance nodes in your StorageGRID system. Each KMS provides a single encryption key to the StorageGRID appliance nodes at a single site or at a group of sites.

StorageGRID supports the use of KMS clusters. Each KMS cluster contains multiple, replicated key management servers that share configuration settings and encryption keys. Using KMS clusters for key management is recommended because it improves the failover capabilities of a high availability configuration.

For example, suppose your StorageGRID system has three data center sites. You might configure one KMS cluster to provide a key to all appliance nodes at Data Center 1 and a second KMS cluster to provide a key to all appliance nodes at all other sites. When you add the second KMS cluster, you can configure a default KMS for Data Center 2 and Data Center 3.

Note that you cannot use a KMS for non-appliance nodes or for any appliance nodes that did not have the **Node Encryption** setting enabled during installation.

Appliance node with node encryption enabled

Appliance node without node encryption enabled

Non-appliance node (not encrypted)
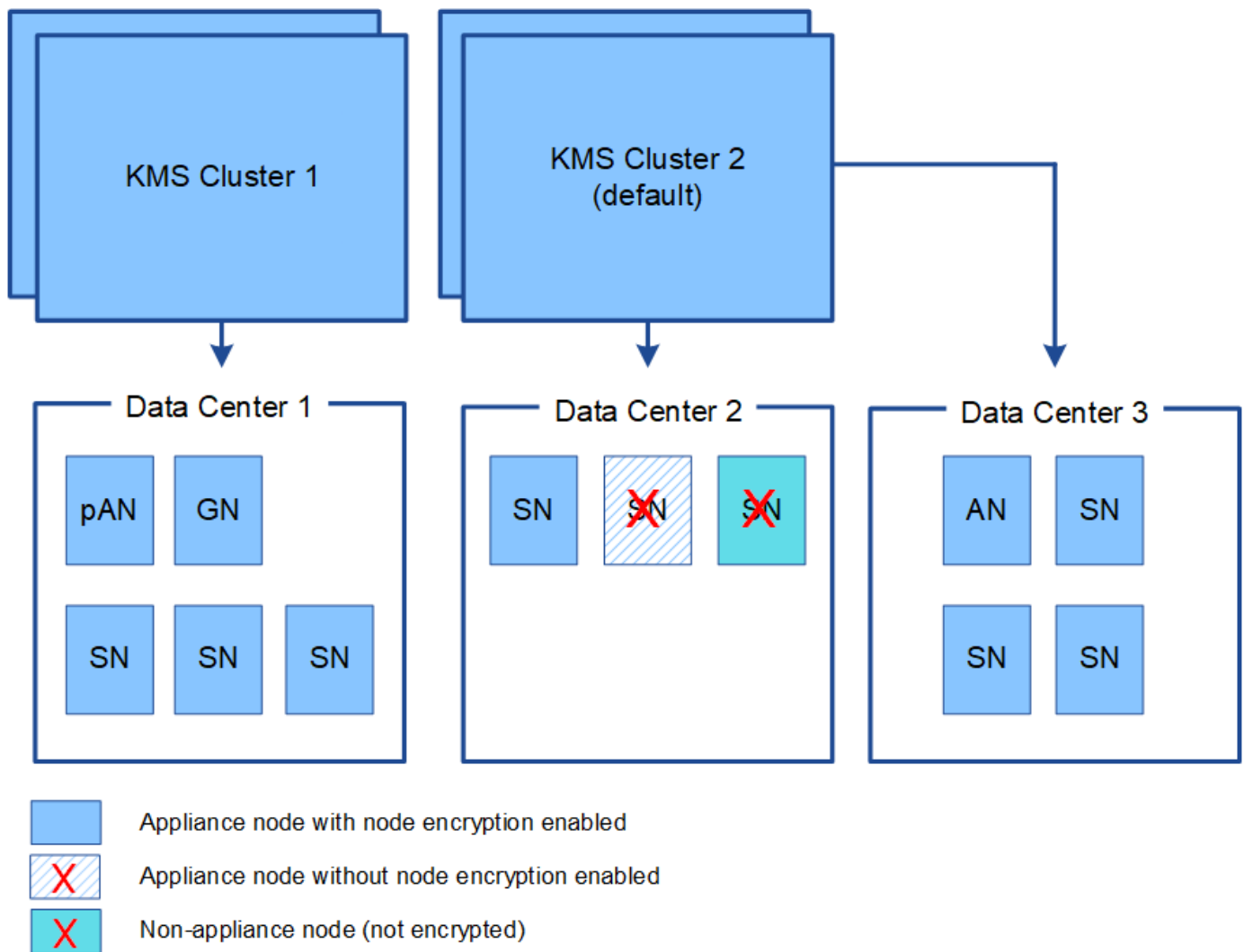
What happens when a key is rotated?

As a security best practice, you should periodically rotate the encryption key used by each configured KMS.

When rotating the encryption key, use the KMS software to rotate from the last used version of the key to a new version of the same key. Do not rotate to an entirely different key.

> ⚠ Never attempt to rotate a key by changing the key name (alias) for the KMS in the Grid Manager. Instead, rotate the key by updating the key version in the KMS software. Use the same key alias for new keys as was used for previous keys. If you change the key alias for a configured KMS, StorageGRID might not be able to decrypt your data.

When the new key version is available:

- It is automatically distributed to the encrypted appliance nodes at the site or sites associated with the KMS. The distribution should occur within an hour of when the key is rotated.
- If the encrypted appliance node is offline when the new key version is distributed, the node will receive the new key as soon as it reboots.
- If the new key version cannot be used to encrypt appliance volumes for any reason, the **KMS encryption key rotation failed** alert is triggered for the appliance node. You might need to contact technical support

for help in resolving this alert.

Can I reuse an appliance node after it has been encrypted?

If you need to install an encrypted appliance into another StorageGRID system, you must first decommission the grid node to move object data to another node. Then, you can use the StorageGRID Appliance Installer to clear the KMS configuration. Clearing the KMS configuration disables the **Node Encryption** setting and removes the association between the appliance node and the KMS configuration for the StorageGRID site.

> (i) With no access to the KMS encryption key, any data that remains on the appliance can no longer be accessed and is permanently locked.

Related information

- SG100 and SG1000 services appliances
- SG6000 storage appliances
- SG5700 storage appliances
- SG5600 storage appliances

Considerations for changing the KMS for a site

Each key management server (KMS) or KMS cluster provides an encryption key to all appliance nodes at a single site or at a group of sites. If you need to change which KMS is used for a site, you might need to copy the encryption key from one KMS to another.

If you change the KMS used for a site, you must ensure that the previously encrypted appliance nodes at that site can be decrypted using the key stored on the new KMS. In some cases, you might need to copy the current version of the encryption key from the original KMS to the new KMS. You must ensure that the KMS has the correct key to decrypt the encrypted appliance nodes at the site.

For example:

1. You initially configure a default KMS that applies to all sites that do not have a dedicated KMS.

2. When the KMS is saved, all appliance nodes that have the **Node Encryption** setting enabled connect to the KMS and request the encryption key. This key is used to encrypt the appliance nodes at all sites. This same key must also be used to decrypt those appliances.
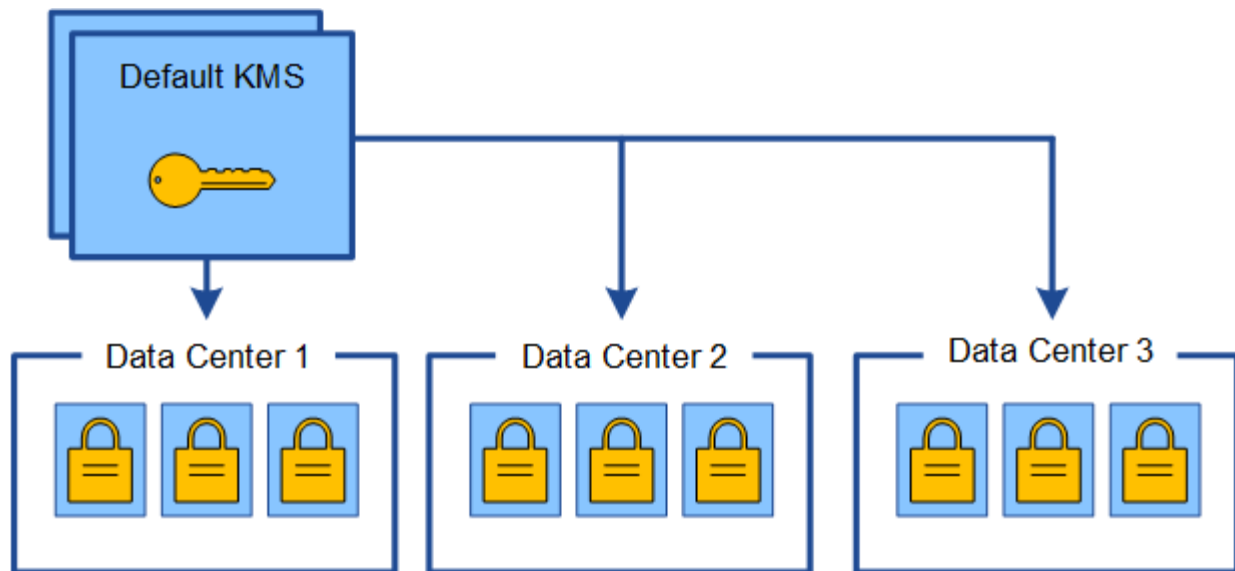
3. You decide to add a site-specific KMS for one site (Data Center 3 in the figure). However, because the appliance nodes are already encrypted, a validation error occurs when you attempt to save the configuration for the site-specific KMS. The error occurs because the site-specific KMS does not have the correct key to decrypt the nodes at that site.
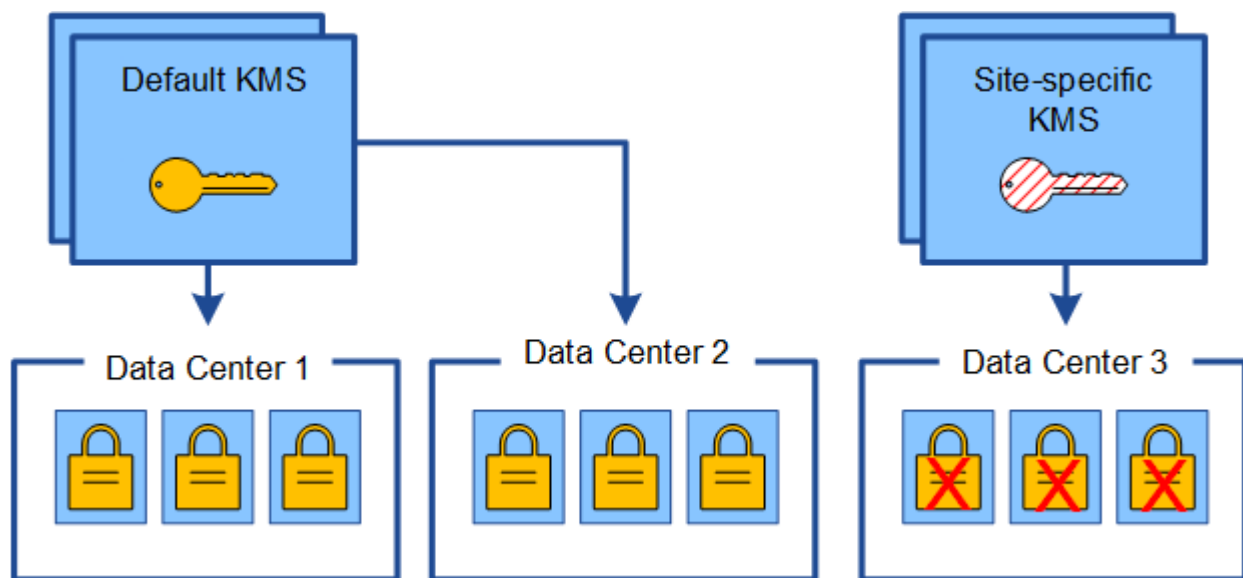
4. To address the issue, you copy the current version of the encryption key from the default KMS to the new KMS. (Technically, you copy the original key to a new key with the same alias. The original key becomes a prior version of the new key.) The site-specific KMS now has the correct key to decrypt the appliance nodes at Data Center 3, so it can be saved in StorageGRID.
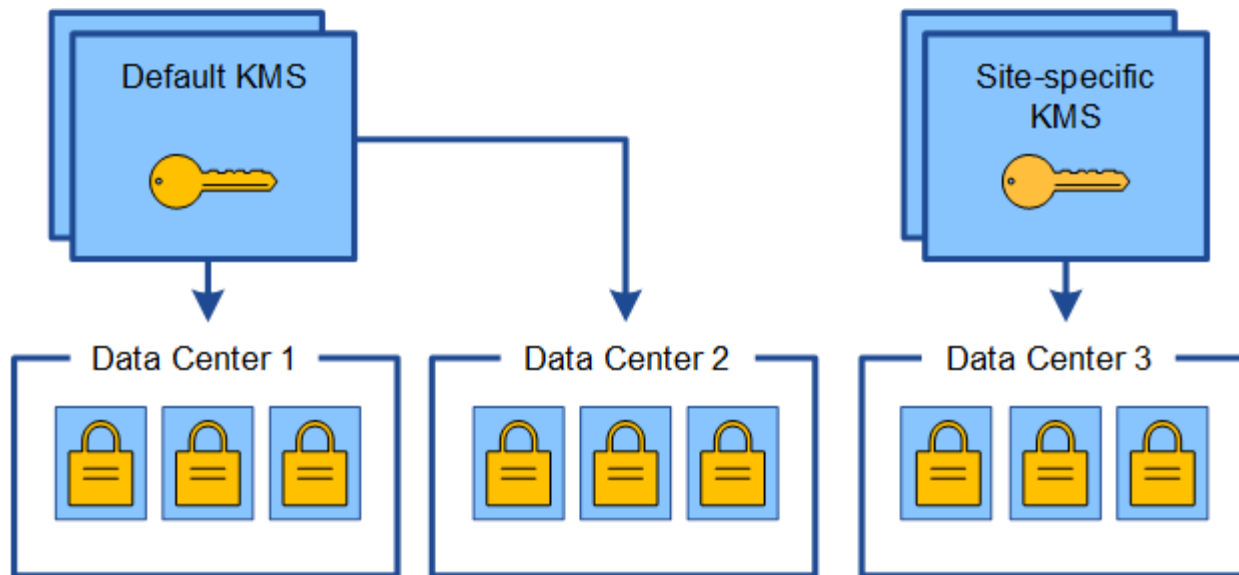
Use cases for changing which KMS is used for a site

The table summarizes the required steps for the most common cases for changing the KMS for a site.

Use case for changing a site's KMS	Required steps
You have one or more site-specific KMS entries, and you want to use one of them as the default KMS.	Edit the site-specific KMS. In the **Manages keys for** field, select **Sites not managed by another KMS (default KMS)**. The site-specific KMS will now be used as the default KMS. It will apply to any sites that do not have a dedicated KMS. Edit a key management server (KMS)
You have a default KMS and you add a new site in an expansion. You do not want to use the default KMS for the new site.	1. If the appliance nodes at the new site have already been encrypted by the default KMS, use the KMS software to copy the current version of the encryption key from the default KMS to a new KMS. 2. Using the Grid Manager, add the new KMS and select the site. Add a key management server (KMS)
You want the KMS for a site to use a different server.	1. If the appliance nodes at the site have already been encrypted by the existing KMS, use the KMS software to copy the current version of the encryption key from the existing KMS to the new KMS. 2. Using the Grid Manager, edit the existing KMS configuration and enter the new host name or IP address. Add a key management server (KMS)

Configure StorageGRID as a client in the KMS

You must configure StorageGRID as a client for each external key management server or KMS cluster before you can add the KMS to StorageGRID.

About this task

These instructions apply to Thales CipherTrust Manager k170v, versions 2.0, 2.1, and 2.2. If you have questions about using a different key management server with StorageGRID, contact technical support.

[Thales CipherTrust Manager](#)

Steps

1. From the KMS software, create a StorageGRID client for each KMS or KMS cluster you plan to use.

   Each KMS manages a single encryption key for the StorageGRID appliances nodes at a single site or at a group of sites.

2. From the KMS software, create an AES encryption key for each KMS or KMS cluster.

   The encryption key needs to be exportable.

3. Record the following information for each KMS or KMS cluster.

   You need this information when you add the KMS to StorageGRID.

   ◦ Host name or IP address for each server.
   ◦ KMIP port used by the KMS.
   ◦ Key alias for the encryption key in the KMS.

   > ⓘ The encryption key must already exist in the KMS. StorageGRID does not create or manage KMS keys.

4. For each KMS or KMS cluster, obtain a server certificate signed by a certificate authority (CA) or a certificate bundle that contains each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

   The server certificate allows the external KMS to authenticate itself to StorageGRID.

   ◦ The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.
   ◦ The Subject Alternative Name (SAN) field in each server certificate must include the fully qualified domain name (FQDN) or IP address that StorageGRID will connect to.

   > ⓘ When you configure the KMS in StorageGRID, you must enter the same FQDNs or IP addresses in the **Hostname** field.

   ◦ The server certificate must match the certificate used by the KMIP interface of the KMS, which typically uses port 5696.

5. Obtain the public client certificate issued to StorageGRID by the external KMS and the private key for the client certificate.

   The client certificate allows StorageGRID to authenticate itself to the KMS.

Add a key management server (KMS)

You use the StorageGRID Key Management Server wizard to add each KMS or KMS cluster.

What you'll need

- You have reviewed the considerations and requirements for using a key management server.

- You have configured StorageGRID as a client in the KMS, and you have the required information for each KMS or KMS cluster.

- You are signed in to the Grid Manager using a supported web browser.

- You have the Root access permission.

About this task

If possible, configure any site-specific key management servers before configuring a default KMS that applies to all sites not managed by another KMS. If you create the default KMS first, all node-encrypted appliances in the grid will be encrypted by the default KMS. If you want to create a site-specific KMS later, you must first copy the current version of the encryption key from the default KMS to the new KMS. See Considerations for changing the KMS for a site for details.

Step 1: Enter KMS Details

In Step 1 (Enter KMS Details) of the Add a Key Management Server wizard, you provide details about the KMS or KMS cluster.

Steps

1. Select **CONFIGURATION** > **Security** > **Key management server**.

   The Key Management Server page appears with the Configuration Details tab selected.

2. Select **Create**.

   Step 1 (Enter KMS Details) of the Add a Key Management Server wizard appears.

Add a Key Management Server

1 Enter KMS Details   **2** Upload Server Certificate   **3** Upload Client Certificates

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name ❓	[ ]
Key Name ❓	[ ]
Manages keys for ❓	-- Choose One -- ▼
Port ❓	5696
Hostname ❓	[ ] +

Cancel   Next

3. Enter the following information for the KMS and the StorageGRID client you configured in that KMS.

Field	Description
KMS Display Name	A descriptive name to help you identify this KMS. Must be between 1 and 64 characters.
Key Name	The exact key alias for the StorageGRID client in the KMS. Must be between 1 and 255 characters.

Field	Description
Manages keys for	The StorageGRID site that will be associated with this KMS. If possible, you should configure any site-specific key management servers before configuring a default KMS that applies to all sites not managed by another KMS. • Select a site if this KMS will manage encryption keys for the appliance nodes at a specific site. • Select **Sites not managed by another KMS (default KMS)** to configure a default KMS that will apply to any sites that do not have a dedicated KMS and to any sites you add in subsequent expansions. **Note:** A validation error will occur when you save the KMS configuration if you select a site that was previously encrypted by the default KMS but you did not provide the current version of original encryption key to the new KMS.
Port	The port the KMS server uses for Key Management Interoperability Protocol (KMIP) communications. Defaults to 5696, which is the KMIP standard port.
Hostname	The fully qualified domain name or IP address for the KMS. **Note:** The SAN field of the server certificate must include the FQDN or IP address you enter here. Otherwise, StorageGRID will not be able to connect to the KMS or to all servers in a KMS cluster.

4. If you are using a KMS cluster, select the plus sign ➕ to add a hostname for each server in the cluster.
5. Select **Next**.

Step 2: Upload Server Certificate

In Step 2 (Upload Server Certificate) of the Add a Key Management Server wizard, you upload the server certificate (or certificate bundle) for the KMS. The server certificate allows the external KMS to authenticate itself to StorageGRID.

Steps

1. From **Step 2 (Upload Server Certificate)**, browse to the location of the saved server certificate or certificate bundle.

Add a Key Management Server

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ❓ | Browse |

| Cancel | Back | Next |

2. Upload the certificate file.

   The server certificate metadata appears.

Add a Key Management Server

① ── ② ── ③

Enter KMS Details — **Upload Server Certificate** — Upload Client Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ❓ [Browse] k170vCA.pem

Server Certficate Metadata

Server DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number:	71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On:	2020-10-15T21:12:45.000Z
Expires On:	2030-10-13T21:12:45.000Z
SHA-1 Fingerprint:	EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79

[Cancel] [Back] [Next]

ⓘ If you uploaded a certificate bundle, the metadata for each certificate appears on its own tab.

3. Select **Next**.

Step 3: Upload Client Certificates

In Step 3 (Upload Client Certificates) of the Add a Key Management Server wizard, you upload the client certificate and the client certificate private key. The client certificate allows StorageGRID to authenticate itself to the KMS.

Steps

1. From **Step 3 (Upload Client Certificates)**, browse to the location of the client certificate.

Add a Key Management Server

1 Enter KMS Details   **2** Upload Server Certificate   **3** Upload Client Certificates

Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ❓   [Browse]

Client Certificate Private Key ❓   [Browse]

[Cancel] [Back] [Save]

2. Upload the client certificate file.

   The client certificate metadata appears.

3. Browse to the location of the private key for the client certificate.

4. Upload the private key file.

   The metadata for the client certificate and the client certificate private key appear.

Add a Key Management Server

Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate [Browse] k170vClientCert.pem

Server DN:	/CN=admin/UID=
Serial Number:	7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On:	2020-10-15T23:31:49.000Z
Expires On:	2022-10-15T23:31:49.000Z
SHA-1 Fingerprint:	A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key [Browse] k170vClientKey.pem

[Cancel] [Back] [Save]

5. Select **Save**.

   The connections between the key management server and the appliance nodes are tested. If all connections are valid and the correct key is found on the KMS, the new key management server is added to the table on the Key Management Server page.

   > ⓘ Immediately after you add a KMS, the certificate status on the Key Management Server page appears as Unknown. It might take StorageGRID as long as 30 minutes to get the actual status of each certificate. You must refresh your web browser to see the current status.

6. If an error message appears when you select **Save**, review the message details and then select **OK**.

   For example, you might receive a 422: Unprocessable Entity error if a connection test failed.

7. If you need to save the current configuration without testing the external connection, select **Force Save**.

Add a Key Management Server

Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Server DN:	/CN=admin/UID=
Serial Number:	7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On:	2020-10-15T23:31:49.000Z
Expires On:	2022-10-15T23:31:49.000Z
SHA-1 Fingerprint:	A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Select Force Save to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Selecting **Force Save** saves the KMS configuration, but it does not test the external connection from each appliance to that KMS. If there is an issue with the configuration, you might not be able to reboot appliance nodes that have node encryption enabled at the affected site. You might lose access to your data until the issues are resolved.

8. Review the confirmation warning, and select **OK** if you are sure you want to force save the configuration.

⚠ Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

The KMS configuration is saved but the connection to the KMS is not tested.

View KMS details

You can view information about each key management server (KMS) in your StorageGRID system, including the current status of the server and client certificates.

Steps

1. Select **CONFIGURATION** > **Security** > **Key management server**.

   The Key Management Server page appears. The Configuration Details tab shows any key management servers that are configured.

   Key Management Server

   If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

   | Configuration Details | Encrypted Nodes |

   You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

   Before adding a KMS:

   * Ensure that the KMS is KMIP-compliant.
   * Configure StorageGRID as a client in the KMS.
   * Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

   For complete instructions, see administering StorageGRID.

+ Create	✎ Edit	⊘ Remove
KMS Display Name ❓	Key Name ❓	Manages keys for ❓	Hostname ❓	Certificate Status ❓
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✔ All certificates are valid

2. Review the information in the table for each KMS.

Field	Description
KMS Display Name	The descriptive name of the KMS.
Key Name	The key alias for the StorageGRID client in the KMS.
Manages keys for	The StorageGRID site associated with the KMS. This field displays the name of a specific StorageGRID site or **Sites not managed by another KMS (default KMS).**

Field	Description
Hostname	The fully qualified domain name or IP address of the KMS. If there is a cluster of two key management servers, the fully qualified domain name or IP address of both servers are listed. If there are more than two key management servers in a cluster, the fully qualified domain name or IP address of the first KMS is listed along with the number of additional key management servers in the cluster. For example: `10.10.10.10 and 10.10.10.11` or `10.10.10.10 and 2 others`. To view all hostnames in a cluster, select a KMS and then select **Edit**.
Certificate Status	Current state of the server certificate, optional CA certificate, and the client certificate: valid, expired, nearing expiration, or unknown. **Note:** It might take StorageGRID as long as 30 minutes to get updates to the certificate status. You must refresh your web browser to see the current values.

3. If the Certificate Status is Unknown, wait up to 30 minutes and then refresh your web browser.

> ⓘ Immediately after you add a KMS, the certificate status on the Key Management Server page appears as Unknown. It might take StorageGRID as long as 30 minutes to get the actual status of each certificate. You must refresh your web browser to see the actual status.

4. If the Certificate Status column indicates that a certificate has expired or is nearing expiration, address the issue as soon as possible.

See the recommended actions for the **KMS CA certificate expiration**, **KMS client certificate expiration**, and **KMS server certificate expiration** alerts in the instructions for monitoring and troubleshooting StorageGRID.

> ⓘ You must address any certificate issues as soon as possible to maintain data access.

View encrypted nodes

You can view information about the appliance nodes in your StorageGRID system that have the **Node Encryption** setting enabled.

Steps

1. Select **CONFIGURATION** > **Security** > **Key management server**.

The Key Management Server page appears. The Configuration Details tab shows any key management servers that have been configured.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

| Configuration Details | Encrypted Nodes |

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see administering StorageGRID.

| + Create | ✎ Edit | ⊘ Remove |

KMS Display Name ❔	Key Name ❔	Manages keys for ❔	Hostname ❔	Certificate Status ❔
⦿ Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✔ All certificates are valid

2. From the top of the page, select the **Encrypted Nodes** tab.

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

| Configuration Details | **Encrypted Nodes** |

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

The Encrypted Nodes tab lists the appliance nodes in your StorageGRID system that have the **Node Encryption** setting enabled.

| Configuration Details | Encrypted Nodes |

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ❔	Key UID ❔	Status ❔
SGA-010-096-104-67 ⬀	Storage Node	Data Center 1	Default KMS	41b0...5c57	✔ Connected to KMS (2021-03-12 10:59:32 MST)

3. Review the information in the table for each appliance node.

Column	Description
Node Name	The name of the appliance node.
Node Type	The type of node: Storage, Admin, or Gateway.

Column	Description
Site	The name of the StorageGRID site where the node is installed.
KMS Display Name	The descriptive name of the KMS used for the node. If no KMS is listed, select the Configuration Details tab to add a KMS. Add a key management server (KMS)
Key UID	The unique ID of the encryption key used to encrypt and decrypt data on the appliance node. To view an entire key UID, hover your cursor over the cell. A dash (--) indicates the key UID is unknown, possibly because of a connection issue between the appliance node and the KMS.
Status	The status of the connection between the KMS and the appliance node. If the node is connected, the timestamp updates every 30 minutes. It can take several minutes for the connection status to update after the KMS configuration changes. **Note:** You must refresh your web browser to see the new values.

4. If the Status column indicates a KMS issue, address the issue immediately.

   During normal KMS operations, the status will be **Connected to KMS**. If a node is disconnected from the grid, the node connection state is shown (Administratively Down or Unknown).

   Other status messages correspond to StorageGRID alerts with the same names:

   - KMS configuration failed to load
   - KMS connectivity error
   - KMS encryption key name not found
   - KMS encryption key rotation failed
   - KMS key failed to decrypt an appliance volume
   - KMS is not configured

   See the recommended actions for these alerts in the instructions for monitoring and troubleshooting StorageGRID.

   ⓘ | You must address any issues immediately to ensure that your data is fully protected.

Edit a key management server (KMS)

You might need to edit the configuration of a key management server, for example, if a certificate is about to expire.

What you'll need

- You have reviewed the considerations and requirements for using a key management server.
- If you plan to update the site selected for a KMS, you have reviewed the considerations for changing the KMS for a site.
- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.

Steps

1. Select **CONFIGURATION** > **Security** > **Key management server**.

   The Key Management Server page appears and shows all key management servers that have been configured.

2. Select the KMS you want to edit, and select **Edit**.

3. Optionally, update the details in **Step 1 (Enter KMS Details)** of the Edit a Key Management Server wizard.

Field	Description
KMS Display Name	A descriptive name to help you identify this KMS. Must be between 1 and 64 characters.

Field	Description
Key Name	The exact key alias for the StorageGRID client in the KMS. Must be between 1 and 255 characters. You only need to edit the key name in rare cases. For example, you must edit the key name if the alias is renamed in the KMS or if all versions of the previous key have been copied to the version history of the new alias. ⚠ Never attempt to rotate a key by changing the key name (alias) for the KMS. Instead, rotate the key by updating the key version in the KMS software. StorageGRID requires all previously used key versions (as well as any future ones) to be accessible from the KMS with the same key alias. If you change the key alias for a configured KMS, StorageGRID might not be able to decrypt your data. Considerations and requirements for using a key management server
Manages keys for	If you are editing a site-specific KMS and you do not already have a default KMS, optionally select **Sites not managed by another KMS (default KMS)**. This selection converts a site-specific KMS to the default KMS, which will apply to all sites that do not have a dedicated KMS and to any sites added in an expansion. **Note:** If you are editing a site-specific KMS, you cannot select another site. If you are editing the default KMS, you cannot select a specific site.
Port	The port the KMS server uses for Key Management Interoperability Protocol (KMIP) communications. Defaults to 5696, which is the KMIP standard port.
Hostname	The fully qualified domain name or IP address for the KMS. **Note:** The SAN field of the server certificate must include the FQDN or IP address you enter here. Otherwise, StorageGRID will not be able to connect to the KMS or to all servers in a KMS cluster.

4. If you are configuring a KMS cluster, select the plus sign ➕ to add a hostname for each server in the cluster.

5. Select **Next**.

   Step 2 (Upload Server Certificate) of the Edit a Key Management Server wizard appears.

6. If you need to replace the server certificate, select **Browse** and upload the new file.

7. Select **Next**.

   Step 3 (Upload Client Certificates) of the Edit a Key Management Server wizard appears.

8. If you need to replace the client certificate and the client certificate private key, select **Browse** and upload the new files.

9. Select **Save**.

   The connections between the key management server and all node-encrypted appliance nodes at the affected sites are tested. If all node connections are valid and the correct key is found on the KMS, the key management server is added to the table on the Key Management Server page.

10. If an error message appears, review the message details, and select **OK**.

    For example, you might receive a 422: Unprocessable Entity error if the site you selected for this KMS is already managed by another KMS, or if a connection test failed.

11. If you need to save the current configuration before resolving the connection errors, select **Force Save**.

    > ⓘ Selecting **Force Save** saves the KMS configuration, but it does not test the external connection from each appliance to that KMS. If there is an issue with the configuration, you might not be able to reboot appliance nodes that have node encryption enabled at the affected site. You might lose access to your data until the issues are resolved.

    The KMS configuration is saved.

12. Review the confirmation warning, and select **OK** if you are sure you want to force save the configuration.

    ⚠ **Warning**

    Confirm force-saving the KMS configuration

    Are you sure you want to save this KMS without testing the external connections?

    If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

    [Cancel] [OK]
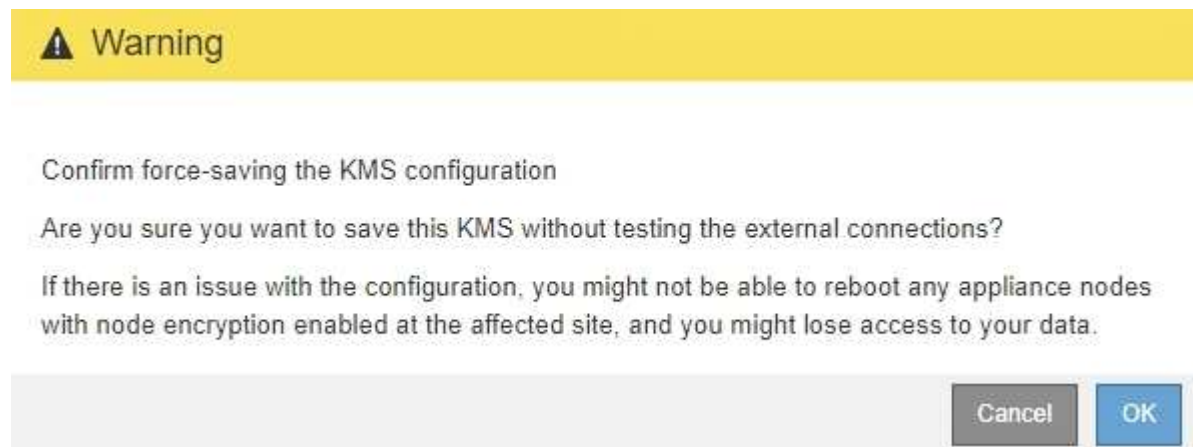
    The KMS configuration is saved but the connection to the KMS is not tested.

Remove a key management server (KMS)

You might want to remove a key management server in some cases. For example, you might want to remove a site-specific KMS if you have decommissioned the site.

What you'll need

- You have reviewed the considerations and requirements for using a key management server.
- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.

About this task

You can remove a KMS in these cases:

- You can remove a site-specific KMS if the site has been decommissioned or if the site includes no appliance nodes with node encryption enabled.
- You can remove the default KMS if a site-specific KMS already exists for each site that has appliance nodes with node encryption enabled.

Steps

1. Select **CONFIGURATION** > **Security** > **Key management server**.

   The Key Management Server page appears and shows all key management servers that have been configured.

   Key Management Server

   If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

   | Configuration Details | Encrypted Nodes |

   You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

   Before adding a KMS:

   - Ensure that the KMS is KMIP-compliant.
   - Configure StorageGRID as a client in the KMS.
   - Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

   For complete instructions, see administering StorageGRID.

   | + Create | ✎ Edit | ⊘ Remove |

KMS Display Name ❔	Key Name ❔	Manages keys for ❔	Hostname ❔	Certificate Status ❔
⦿ Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✔ All certificates are valid

2. Select the radio button for the KMS you want to remove, and select **Remove**.

3. Review the considerations in the warning dialog.

   ⚠ **Warning**

   Delete KMS Configuration

   You can only remove a KMS in these cases:

   - You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
   - You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

   Are you sure you want to delete the Default KMS KMS configuration?

   | Cancel | OK |

4. Select **OK**.

   The KMS configuration is removed.

Copyright Information

Trademark Information