



# **Manage security settings**

## **StorageGRID**

NetApp  
April 10, 2024

# Table of Contents

- Manage security settings ..... 1
  - Manage certificates ..... 1
  - Configure key management servers ..... 30
  - Manage proxy settings ..... 59
  - Manage untrusted Client Networks ..... 61

# Manage security settings

## Manage certificates

### About security certificates

Security certificates are small data files used to create secure, trusted connections between StorageGRID components and between StorageGRID components and external systems.

StorageGRID uses two types of security certificates:

- **Server certificates** are required when you use HTTPS connections. Server certificates are used to establish secure connections between clients and servers, authenticating the identity of a server to its clients and providing a secure communication path for data. The server and the client each have a copy of the certificate.
- **Client certificates** authenticate a client or user identity to the server, providing more secure authentication than passwords alone. Client certificates do not encrypt data.

When a client connects to the server using HTTPS, the server responds with the server certificate, which contains a public key. The client verifies this certificate by comparing the server signature to the signature on its copy of the certificate. If the signatures match, the client starts a session with the server using the same public key.

StorageGRID functions as the server for some connections (such as the load balancer endpoint) or as the client for other connections (such as the CloudMirror replication service).

### Default Grid CA certificate

StorageGRID includes a built-in certificate authority (CA) that generates an internal Grid CA certificate during system installation. The Grid CA certificate is used, by default, to secure internal StorageGRID traffic. An external certificate authority (CA) can issue custom certificates that are fully compliant with your organization's information security policies. Although you can use the Grid CA certificate for a non-production environment, the best practice for a production environment is to use custom certificates signed by an external certificate authority. Unsecured connections with no certificate are also supported but are not recommended.

- Custom CA certificates do not remove the internal certificates; however, the custom certificates should be the ones specified for verifying server connections.
- All custom certificates must meet the [system hardening guidelines](#) for server certificates.
- StorageGRID supports bundling of certificates from a CA into a single file (known as a CA certificate bundle).



StorageGRID also includes operating system CA certificates that are the same on all grids. In production environments, make sure that you specify a custom certificate signed by an external certificate authority in place of the operating system CA certificate.

Variants of the server and client certificate types are implemented in several ways. You should have all the certificates needed for your specific StorageGRID configuration ready before you configure the system.

## Access security certificates

You can access information about all StorageGRID certificates in a single location, along with links to the configuration workflow for each certificate.

1. From Grid Manager, select **CONFIGURATON > Security > Certificates**.

# Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ?	Expiration date ? ↕
<a href="#">Management interface certificate</a>	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
<a href="#">S3 and Swift API certificate</a>	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Select a tab on the Certificates page for information about each certificate category and to access the certificate settings. You can only access a tab if you have the appropriate permission.
  - **Global:** Secures StorageGRID access from web browsers and external API clients.
  - **Grid CA:** Secures internal StorageGRID traffic.
  - **Client:** Secures connections between external clients and the StorageGRID Prometheus database.
  - **Load balancer endpoints:** Secures connections between S3 and Swift clients and the StorageGRID Load Balancer.
  - **Tenants:** Secures connections to identity federation servers or from platform service endpoints to S3 storage resources.
  - **Other:** Secures StorageGRID connections requiring specific certificates.

Each tab is described below with links to additional certificate details.

## Global

The global certificates secure StorageGRID access from web browsers and external S3 and Swift API clients. Two global certificates are initially generated by the StorageGRID certificate authority during installation. The best practice for a production environment is to use custom certificates signed by an external certificate authority.

- [Management interface certificate](#): Secures client web-browser connections to StorageGRID management interfaces.
- [S3 and Swift API certificate](#): Secures client API connections to Storage Nodes, Admin Nodes, and Gateway Nodes, which S3 and Swift client applications use to upload and download object data.

Information about the global certificates that are installed includes:

- **Name**: Certificate name with link to managing the certificate.
- **Description**
- **Type**: Custom or default.  
You should always use a custom certificate for improved grid security.
- **Expiration date**: If using the default certificate, no expiration date is shown.

You can:

- Replace the default certificates with custom certificates signed by an external certificate authority for improved grid security:
  - [Replace the default StorageGRID-generated management interface certificate](#) used for Grid Manager and Tenant Manager connections.
  - [Replace the S3 and Swift API certificate](#) used for Storage Node, CLB service (deprecated), and load balancer endpoint (optional) connections.
- [Restore the default management interface certificate](#).
- [Restore the default S3 and Swift API certificate](#).
- [Use a script to generate a new self-signed management interface certificate](#).
- Copy or download the [management interface certificate](#) or [S3 and Swift API certificate](#).

## Grid CA

The [Grid CA certificate](#), generated by the StorageGRID certificate authority during StorageGRID installation, secures all internal StorageGRID traffic.

Certificate information includes the certificate expiration date and the certificate contents.

You can [Copy or download the Grid CA certificate](#), but you cannot change it.

## Client

[Client certificates](#), generated by an external certificate authority, secure the connections between external monitoring tools and the StorageGRID Prometheus database.

The certificate table has a row for each configured client certificate and indicates whether the certificate can be used for Prometheus database access, along with the certificate expiration date.

You can:

- [Upload or generate a new client certificate.](#)
- Select a certificate name to display the certificate details where you can:
  - [Change the client certificate name.](#)
  - [Set the Prometheus access permission.](#)
  - [Upload and replace the client certificate.](#)
  - [Copy or download the client certificate.](#)
  - [Remove the client certificate.](#)
- Select **Actions** to quickly [edit](#), [attach](#), or [remove](#) a client certificate. You can select up to 10 client certificates and remove them at one time using **Actions > Remove**.

### Load balancer endpoints

[Load balancer endpoint certificates](#), that you upload or generate, secure the connections between S3 and Swift clients and the StorageGRID Load Balancer service on Gateway Nodes and Admin Nodes.

The load balancer endpoint table has a row for each configured load balancer endpoint and indicates whether the global S3 and Swift API certificate or a custom load balancer endpoint certificate is being used for the endpoint. The expiration date for each certificate is also displayed.



Changes to an endpoint certificate can take up to 15 minutes to be applied to all nodes.

You can:

- [Select an endpoint name to open a browser tab with information about the load balancer endpoint, including its certificate details.](#)
- [Specify a load balancer endpoint certificate for FabricPool.](#)
- [Use the global S3 and Swift API certificate](#) instead of generating a new load balancer endpoint certificate.

### Tenants

Tenants can use [identity federation server certificates](#) or [platform service endpoint certificates](#) to secure their connections with StorageGRID.

The tenant table has a row for each tenant and indicates if each tenant has permission to use its own identity source or platform services.

You can:

- [Select a tenant name to sign in to the Tenant Manager](#)
- [Select a tenant name to view the tenant identity federation details](#)
- [Select a tenant name to view tenant platform services details](#)
- [Specify a platform service endpoint certificate during endpoint creation](#)

### Other

StorageGRID uses other security certificates for specific purposes. These certificates are listed by their functional name. Other security certificates include:

- [Identity federation certificates](#)

- [Cloud Storage Pool certificates](#)
- [Key management server \(KMS\) certificates](#)
- [Single sign-on certificates](#)
- [Email alert notification certificates](#)
- [External syslog server certificates](#)

Information indicates the type of certificate a function uses and its server and client certificate expiration dates, as applicable. Selecting a function name opens a browser tab where you can view and edit the certificate details.



You can only view and access information for other certificates if you have the appropriate permission.

You can:

- [View and edit an identity federation certificate](#)
- [Upload key management server \(KMS\) server and client certificates](#)
- [Specify a Cloud Storage Pool certificate for S3, C2S S3, or Azure](#)
- [Manually specify an SSO certificate for relying party trust](#)
- [Specify a certificate for alert email notifications](#)
- [Specify an external syslog server certificate](#)

## Security certificate details

Each type of security certificate is described below, with links to articles that contain implementation instructions.

### Management interface certificate

Certificate type	Description	Navigation location	Details
Server	<p>Authenticates the connection between client web browsers and the StorageGRID management interface, allowing users to access the Grid Manager and Tenant Manager without security warnings.</p> <p>This certificate also authenticates Grid Management API and Tenant Management API connections.</p> <p>You can use the default certificate created during installation or upload a custom certificate.</p>	<b>CONFIGURATION &gt; Security &gt; Certificates</b> , select the <b>Global</b> tab, and then select <b>Management interface certificate</b>	<a href="#">Configure management interface certificates</a>

#### S3 and Swift API certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates secure S3 or Swift client connections to a Storage Node, to the deprecated Connection Load Balancer (CLB) service on a Gateway Node, and load balancer endpoints (optional).	<b>CONFIGURATION &gt; Security &gt; Certificates</b> , select the <b>Global</b> tab, and then select <b>S3 and Swift API certificate</b>	<a href="#">Configure S3 and Swift API certificates</a>

#### Grid CA certificate

See the [Default Grid CA certificate description](#).

#### Administrator client certificate



Certificate type	Description	Navigation location	Details
Client	<p>Installed on each client, allowing StorageGRID to authenticate external client access.</p> <ul style="list-style-type: none"> <li>• Allows authorized external clients to access the StorageGRID Prometheus database.</li> <li>• Allows secure monitoring of StorageGRID using external tools.</li> </ul>	<b>CONFIGURATION &gt; Security &gt; Certificates</b> and then select the <b>Client</b> tab	<a href="#">Configure client certificates</a>

#### Load balancer endpoint certificate

Certificate type	Description	Navigation location	Details
Server	<p>Authenticates the connection between S3 or Swift clients and the StorageGRID Load Balancer service on Gateway Nodes and Admin Nodes. You can upload or generate a load balancer certificate when you configure a load balancer endpoint. Client applications use the load balancer certificate when connecting to StorageGRID to save and retrieve object data.</p> <p>You can also use a custom version of the global <a href="#">S3 and Swift API certificate</a> to authenticate connections to the Load Balancer service. If the global certificate is used to authenticate load balancer connections, you do not need to upload or generate a separate certificate for each load balancer endpoint.</p> <p><b>Note:</b> The certificate used for load balancer authentication is the most used certificate during normal StorageGRID operation.</p>	<b>CONFIGURATION &gt; Network &gt; Load balancer endpoints</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configure load balancer endpoints</a></li> <li>• <a href="#">Create a load balancer endpoint for FabricPool</a></li> </ul>

#### Identity federation certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between StorageGRID and an external identity provider, such as Active Directory, OpenLDAP, or Oracle Directory Server. Used for identity federation, which allows admin groups and users to be managed by an external system.	<b>CONFIGURATION &gt; Access Control &gt; Identity federation</b>	<a href="#">Use identity federation</a>

#### Platform services endpoint certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection from the StorageGRID platform service to an S3 storage resource.	<b>Tenant Manager &gt; STORAGE (S3) &gt; Platform services endpoints</b>	<a href="#">Create platform services endpoint</a>  <a href="#">Edit platform services endpoint</a>

#### Cloud Storage Pool endpoint certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection from a StorageGRID Cloud Storage Pool to an external storage location, such as S3 Glacier or Microsoft Azure Blob storage. A different certificate is required for each cloud provider type.	<b>ILM &gt; Storage pools</b>	<a href="#">Create a Cloud Storage Pool</a>

#### Key management server (KMS) certificate

Certificate type	Description	Navigation location	Details
Server and client	Authenticates the connection between StorageGRID and an external key management server (KMS), which provides encryption keys to StorageGRID appliance nodes.	<b>CONFIGURATION &gt; Security &gt; Key management server</b>	<a href="#">Add key management server (KMS)</a>

#### Single sign-on (SSO) certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between identity federation services, such as Active Directory Federation Services (AD FS), and StorageGRID that are used for single sign-on (SSO) requests.	<b>CONFIGURATION &gt; Access control &gt; Single sign-on</b>	<a href="#">Configure single sign-on</a>

#### Email alert notification certificate

Certificate type	Description	Navigation location	Details
Server and client	<p>Authenticates the connection between an SMTP email server and StorageGRID that is used for alert notifications.</p> <ul style="list-style-type: none"><li>• If communications with the SMTP server requires Transport Layer Security (TLS), you must specify the email server CA certificate.</li><li>• Specify a client certificate only if the SMTP email server requires client certificates for authentication.</li></ul>	<b>ALERTS &gt; Email setup</b>	<a href="#">Set up email notifications for alerts</a>

#### External syslog server certificate

Certificate type	Description	Navigation location	Details
Server	<p>Authenticates the TLS or RELP/TLS connection between an external syslog server that logs events in StorageGRID.</p> <p><b>Note:</b> An external syslog server certificate is not required for TCP, RELP/TCP, and UDP connections to an external syslog server.</p>	<b>CONFIGURATION &gt; Monitoring &gt; Audit and syslog server</b> and then select <b>Configure external syslog server</b>	<a href="#">Configure an external syslog server</a>

## Certificate examples

### Example 1: Load Balancer service

In this example, StorageGRID acts as the server.

1. You configure a load balancer endpoint and upload or generate a server certificate in StorageGRID.
2. You configure an S3 or Swift client connection to the load balancer endpoint and upload the same certificate to the client.
3. When the client wants to save or retrieve data, it connects to the load balancer endpoint using HTTPS.
4. StorageGRID responds with the server certificate, which contains a public key, and with a signature based on the private key.
5. The client verifies this certificate by comparing the server signature to the signature on its copy of the certificate. If the signatures match, the client starts a session using the same public key.
6. The client sends object data to StorageGRID.

### Example 2: External key management server (KMS)

In this example, StorageGRID acts as the client.

1. Using external Key Management Server software, you configure StorageGRID as a KMS client and obtain a CA-signed server certificate, a public client certificate, and the private key for the client certificate.
2. Using the Grid Manager, you configure a KMS server and upload the server and client certificates and the client private key.
3. When a StorageGRID node needs an encryption key, it makes a request to the KMS server that includes data from the certificate and a signature based on the private key.
4. The KMS server validates the certificate signature and decides that it can trust StorageGRID.
5. The KMS server responds using the validated connection.

## Configure server certificates

### Supported server certificate types

The StorageGRID system supports custom certificates encrypted with RSA or ECDSA

## (Elliptic Curve Digital Signature Algorithm).

For more information on how StorageGRID secures client connections for the REST API, see [Use S3](#) or [Use Swift](#).

### Configure management interface certificates

You can replace the default management interface certificate with a single custom certificate that allows users to access the Grid Manager and the Tenant Manager without encountering security warnings. You can also revert to the default management interface certificate or generate a new one.

#### About this task

By default, every Admin Node is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom management interface certificate and corresponding private key.

Because a single custom management interface certificate is used for all Admin Nodes, you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the Grid Manager and Tenant Manager. Define the custom certificate such that it matches all Admin Nodes in the grid.

You need to complete configuration on the server, and depending on the root certificate authority (CA) you are using, users might also need to install the Grid CA certificate in the web browser they will use to access the Grid Manager and the Tenant Manager.



To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Management Interface** alert is triggered when this server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION > Security > Certificates** and looking at the Expiration date for the management interface certificate on the Global tab.



If you are accessing the Grid Manager or Tenant Manager using a domain name instead of an IP address, the browser shows a certificate error without an option to bypass if either of the following occurs:

- Your custom management interface certificate expires.
- You [revert from a custom management interface certificate to the default server certificate](#).

### Add a custom management interface certificate

To add a custom management interface certificate, you can provide your own certificate or generate one using the Grid Manager.

#### Steps

1. Select **CONFIGURATION > Security > Certificates**.
2. On the **Global** tab, select **Management interface certificate**.
3. Select **Use custom certificate**.
4. Upload or generate the certificate.

## Upload certificate

Upload the required server certificate files.

1. Select **Upload certificate**.
2. Upload the required server certificate files:
  - **Server certificate**: The custom server certificate file (PEM encoded).
  - **Certificate private key**: The custom server certificate private key file (.key).



EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

- **CA bundle**: A single optional file containing the certificates from each intermediate issuing certificate authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
3. Expand **Certificate details** to see the metadata for each certificate you uploaded. If you uploaded an optional CA bundle, each certificate displays on its own tab.
    - Select **Download certificate** to save the certificate file or select **Download CA bundle** to save the certificate bundle.

Specify the certificate file name and download location. Save the file with the extension .pem.

For example: storagegrid\_certificate.pem

- Select **Copy certificate PEM** or **Copy CA bundle PEM** to copy the certificate contents for pasting elsewhere.
4. Select **Save**.

The custom management interface certificate is used for all subsequent new connections to the Grid Manager, Tenant Manager, Grid Manager API or Tenant Manager API.

## Generate certificate

Generate the server certificate files.



The best practice for a production environment is to use a custom management interface certificate signed by an external certificate authority.

1. Select **Generate certificate**.
2. Specify the certificate information:
  - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an \* as a wildcard to represent multiple domain names.
  - **IP**: One or more IP addresses to include in the certificate.
  - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
  - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Certificate details** to see the metadata for the generated certificate.
  - Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.

5. Select **Save**.

The custom management interface certificate is used for all subsequent new connections to the Grid Manager, Tenant Manager, Grid Manager API or Tenant Manager API.

5. Refresh the page to ensure the web browser is updated.



After uploading or generating a new certificate, allow up to one day for any related certificate expiration alerts to clear.

6. After you add a custom management interface certificate, the Management interface certificate page displays detailed certificate information for the certificates that are in use. You can download or copy the certificate PEM as required.

### Restore the default management interface certificate

You can revert to using the default management interface certificate for Grid Manager and Tenant Manager connections.

#### Steps

1. Select **CONFIGURATION > Security > Certificates**.
2. On the **Global** tab, select **Management interface certificate**.
3. Select **Use default certificate**.

When you restore the default management interface certificate, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default management interface certificate is used for all subsequent new client connections.

4. Refresh the page to ensure the web browser is updated.

### Use a script to generate a new self-signed management interface certificate

If strict hostname validation is required, you can use a script to generate the management interface certificate.

#### What you'll need

- You have specific access permissions.
- You have the `Passwords.txt` file.

#### About this task

The best practice for a production environment is to use a certificate signed by an external certificate authority.

#### Steps

1. Obtain the fully qualified domain name (FQDN) of each Admin Node.
2. Log in to the primary Admin Node:
  - a. Enter the following command: `ssh admin@primary_Admin_Node_IP`



- b. Enter the password listed in the `Passwords.txt` file.
- c. Enter the following command to switch to root: `su -`
- d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

### 3. Configure StorageGRID with a new self-signed certificate.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- For `--domains`, use wildcards to represent the fully qualified domain names of all Admin Nodes. For example, `*.ui.storagegrid.example.com` uses the `*` wildcard to represent `admin1.ui.storagegrid.example.com` and `admin2.ui.storagegrid.example.com`.
- Set `--type` to `management` to configure the management interface certificate, which is used by Grid Manager and Tenant Manager.
- By default, generated certificates are valid for one year (365 days) and must be recreated before they expire. You can use the `--days` argument to override the default validity period.



A certificate's validity period begins when `make-certificate` is run. You must ensure the management client is synchronized to the same time source as StorageGRID; otherwise, the client might reject the certificate.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

The resulting output contains the public certificate needed by your management API client.

### 4. Select and copy the certificate.

Include the `BEGIN` and the `END` tags in your selection.

### 5. Log out of the command shell. `$ exit`

### 6. Confirm the certificate was configured:

- a. Access the Grid Manager.
- b. Select **CONFIGURATION > Security > Certificates**
- c. On the **Global** tab, select **Management interface certificate**.

### 7. Configure your management client to use the public certificate you copied. Include the `BEGIN` and `END` tags.

#### Download or copy the management interface certificate

You can save or copy the management interface certificate contents for use elsewhere.

#### Steps

1. Select **CONFIGURATION > Security > Certificates**.
2. On the **Global** tab, select **Management interface certificate**.

3. Select the **Server** or **CA bundle** tab and then download or copy the certificate.

#### **Download certificate file or CA bundle**

Download the certificate or CA bundle `.pem` file. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

1. Select **Download certificate** or **Download CA bundle**.

If you are downloading a CA bundle, all the certificates in the CA bundle secondary tabs download as a single file.

2. Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

#### **Copy certificate or CA bundle PEM**

Copy the certificate text to paste elsewhere. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

1. Select **Copy certificate PEM** or **Copy CA bundle PEM**.

If you are copying a CA bundle, all the certificates in the CA bundle secondary tabs copy together.

2. Paste the copied certificate into a text editor.
3. Save the text file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

### **Configure S3 and Swift API certificates**

You can replace or restore the server certificate that is used for S3 or Swift client connections to Storage Nodes, the deprecated Connection Load Balancer (CLB) service on Gateway Nodes, or to load balancer endpoints. The replacement custom server certificate is specific to your organization.

#### **About this task**

By default, every Storage Node is issued a X.509 server certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

A single custom server certificate is used for all Storage Nodes, so you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the storage endpoint. Define the custom certificate such that it matches all Storage Nodes in the grid.

After completing configuration on the server, you might also need to install the Grid CA certificate in the S3 or Swift API client you will use to access the system, depending on the root certificate authority (CA) you are using.



To ensure that operations are not disrupted by a failed server certificate, the **Expiration of global server certificate for S3 and Swift API** alert is triggered when the root server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION > Security > Certificates** and looking at the Expiration date for the S3 and Swift API certificate on the Global tab.

You can upload or generate a custom S3 and Swift API certificate.

#### **Add a custom S3 and Swift API certificate**

##### **Steps**

1. Select **CONFIGURATION > Security > Certificates**.
2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select **Use custom certificate**.
4. Upload or generate the certificate.

## Upload certificate

Upload the required server certificate files.

1. Select **Upload certificate**.
2. Upload the required server certificate files:
  - **Server certificate**: The custom server certificate file (PEM encoded).
  - **Certificate private key**: The custom server certificate private key file (.key).



EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

- **CA bundle**: A single optional file containing the certificates from each intermediate issuing certificate authority. The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
3. Select the certificate details to display the metadata and PEM for each custom S3 and Swift API certificate that was uploaded. If you uploaded an optional CA bundle, each certificate displays on its own tab.
    - Select **Download certificate** to save the certificate file or select **Download CA bundle** to save the certificate bundle.

Specify the certificate file name and download location. Save the file with the extension .pem.

For example: `storagegrid_certificate.pem`

- Select **Copy certificate PEM** or **Copy CA bundle PEM** to copy the certificate contents for pasting elsewhere.
4. Select **Save**.

The custom server certificate is used for subsequent new S3 and Swift client connections.

## Generate certificate

Generate the server certificate files.

1. Select **Generate certificate**.
2. Specify the certificate information:
  - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an \* as a wildcard to represent multiple domain names.
  - **IP**: One or more IP addresses to include in the certificate.
  - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
  - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Certificate Details** to display the metadata and PEM for the custom S3 and Swift API certificate that was generated.
  - Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.

5. Select **Save**.

The custom server certificate is used for subsequent new S3 and Swift client connections.

5. Select a tab to display metadata for the default StorageGRID server certificate, a CA signed certificate that was uploaded, or a custom certificate that was generated.



After uploading or generating a new certificate, allow up to one day for any related certificate expiration alerts to clear.

6. Refresh the page to ensure the web browser is updated.

7. After you add a custom S3 and Swift API certificate the S3 and Swift API certificate page displays detailed certificate information for the custom S3 and Swift API certificate that is in use.

You can download or copy the certificate PEM as required.

#### Restore the default S3 and Swift API certificate

You can revert to using the default S3 and Swift API certificate for S3 and Swift client connections to Storage Nodes and to the deprecated CLB service on Gateway Nodes. However, you cannot use the default S3 and Swift API certificate for a load balancer endpoint.

#### Steps

1. Select **CONFIGURATION > Security > Certificates**.
2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select **Use default certificate**.

When you restore the default version of the global S3 and Swift API certificate, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default S3 and Swift API certificate will be used for subsequent new S3 and Swift client connections to Storage Nodes and to the deprecated CLB service on Gateway Nodes.

4. Select **OK** to confirm the warning and restore the default S3 and Swift API certificate.

If you have Root access permission and the custom S3 and Swift API certificate was used for load balancer endpoint connections, a list is displayed of load balancer endpoints that will no longer be accessible using the default S3 and Swift API certificate. Go to [Configure load balancer endpoints](#) to edit or remove the affected endpoints.

5. Refresh the page to ensure the web browser is updated.

#### Download or copy the S3 and Swift API certificate

You can save or copy the S3 and Swift API certificate contents for use elsewhere.

#### Steps

1. Select **CONFIGURATION > Security > Certificates**.

2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select the **Server** or **CA bundle** tab and then download or copy the certificate.

#### Download certificate file or CA bundle

Download the certificate or CA bundle .pem file. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

- a. Select **Download certificate** or **Download CA bundle**.

If you are downloading a CA bundle, all the certificates in the CA bundle secondary tabs download as a single file.

- b. Specify the certificate file name and download location. Save the file with the extension .pem.

For example: storagegrid\_certificate.pem

#### Copy certificate or CA bundle PEM

Copy the certificate text to paste elsewhere. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

- a. Select **Copy certificate PEM** or **Copy CA bundle PEM**.

If you are copying a CA bundle, all the certificates in the CA bundle secondary tabs copy together.

- b. Paste the copied certificate into a text editor.
- c. Save the text file with the extension .pem.

For example: storagegrid\_certificate.pem

#### Related information

- [Use S3](#)
- [Use Swift](#)
- [Configure S3 API endpoint domain names](#)

#### Copy the Grid CA certificate

StorageGRID uses an internal certificate authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

#### What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have specific access permissions.

#### About this task

If a custom server certificate has been configured, client applications should verify the server using the custom server certificate. They should not copy the CA certificate from the StorageGRID system.

## Steps

1. Select **CONFIGURATION > Security > Certificates** and then select the **Grid CA** tab.
2. In the **Certificate PEM** section download or copy the certificate.

### Download certificate file

Download the certificate .pem file.

1. Select **Download certificate**.
2. Specify the certificate file name and download location. Save the file with the extension .pem.

For example: `storagegrid_certificate.pem`

### Copy certificate PEM

Copy the certificate text to paste elsewhere.

1. Select **Copy certificate PEM**.
2. Paste the copied certificate into a text editor.
3. Save the text file with the extension .pem.

For example: `storagegrid_certificate.pem`

## Configure StorageGRID certificates for FabricPool

For S3 clients that perform strict hostname validation and do not support disabling strict hostname validation, such as ONTAP clients using FabricPool, you can generate or upload a server certificate when you configure the load balancer endpoint.

### What you'll need

- You have specific access permissions.
- You are signed in to the Grid Manager using a [supported web browser](#).

### About this task

When you create a load balancer endpoint, you can generate a self-signed server certificate or upload a certificate that is signed by a known certificate authority (CA). In production environments, you should use a certificate that is signed by a known CA. Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

The following steps provide general guidelines for S3 clients that use FabricPool. For more detailed information and procedures, see [Configure StorageGRID for FabricPool](#).



The separate Connection Load Balancer (CLB) service on Gateway Nodes is deprecated and not recommended for use with FabricPool.

## Steps

1. Optionally, configure a high availability (HA) group for FabricPool to use.

2. Create an S3 load balancer endpoint for FabricPool to use.

When you create an HTTPS load balancer endpoint, you are prompted to upload your server certificate, certificate private key, and optional CA bundle.

3. Attach StorageGRID as a cloud tier in ONTAP.

Specify the load balancer endpoint port and the fully qualified domain name used in the CA certificate you uploaded. Then, provide the CA certificate.



If an intermediate CA issued the StorageGRID certificate, you must provide the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, you must provide the Root CA certificate.

## Configure client certificates

Client certificates allow authorized external clients to access the StorageGRID Prometheus database, providing a secure way for external tools to monitor StorageGRID.

If you need to access StorageGRID using an external monitoring tool, you must upload or generate a client certificate using the Grid Manager and copy the certificate information to the external tool.

See the information about [general security certificate use](#) and [configuring custom server certificates](#).



To ensure that operations are not disrupted by a failed server certificate, the **Expiration of client certificates configured on the Certificates page** alert is triggered when this server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION > Security > Certificates** and looking at the Expiration date for the client certificate on the Client tab.



If you are using a key management server (KMS) to protect the data on specially configured appliance nodes, see the specific information about [uploading a KMS client certificate](#).

### What you'll need

- You have Root access permission.
- You are signed in to the Grid Manager using a [supported web browser](#).
- To configure a client certificate:
  - You have the IP address or domain name of the Admin Node.
  - If you have configured the StorageGRID management interface certificate, you have the CA, client certificate, and private key used to configure the management interface certificate.
  - To upload your own certificate, the private key for the certificate is available on your local computer.
  - The private key must have been saved or recorded at the time it was created. If you do not have the original private key, you must create a new one.
- To edit a client certificate:
  - You have the IP address or domain name of the Admin Node.
  - To upload your own certificate or a new certificate, the private key, client certificate, and CA (if used) are available on your local computer.



## Add client certificates

Follow the procedure for your scenario to add a client certificate:

- [Management interface certificate already configured](#)
- [CA issued client certificate](#)
- [Generated certificate from Grid Manager](#)

### Management interface certificate already configured

Use this procedure to add a client certificate if a management interface certificate is already configured using a customer-supplied CA, client certificate, and private key.

#### Steps

1. In the Grid Manager, select **CONFIGURATION > Security > Certificates** and then select the **Client** tab.
2. Select **Add**.
3. Enter a certificate name that contains at least 1 and no more than 32 characters.
4. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
5. In the **Certificate type** section, upload the management interface certificate .pem file.
  - a. Select **Upload certificate** and then select **Continue**.
  - b. Upload the management interface certificate file (.pem).
    - Select **Client certificate details** to display the certificate metadata and certificate PEM.
    - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
  - c. Select **Create** to save the certificate in the Grid Manager.

The new certificate appears on the Client tab.

6. Configure the following settings on your external monitoring tool, such as Grafana.
  - a. **Name:** Enter a name for the connection.

StorageGRID does not require this information, but you must provide a name to test the connection.
  - b. **URL:** Enter the domain name or IP address for the Admin Node. Specify HTTPS and port 9091.

For example: `https://admin-node.example.com:9091`
  - c. Enable **TLS Client Auth** and **With CA Cert**.
  - d. Under TLS/SSL Auth Details, copy and paste:
    - The management interface CA certificate to **CA Cert**
    - The client certificate to **Client Cert**
    - The private key to **Client Key**
  - e. **ServerName:** Enter the domain name of the Admin Node.

ServerName must match the domain name as it appears in the management interface certificate.

- f. Save and test the certificate and private key that you copied from StorageGRID or a local file.

You can now access the Prometheus metrics from StorageGRID with your external monitoring tool.

For information about the metrics, see the [instructions for monitoring StorageGRID](#).

### CA issued client certificate

Use this procedure to add an administrator client certificate if a management interface certificate was not configured and you plan to add a client certificate for Prometheus that uses a CA issued client certificate and private key.

#### Steps

1. Perform the steps to [configure a management interface certificate](#).
2. In the Grid Manager, select **CONFIGURATION > Security > Certificates** and then select the **Client** tab.
3. Select **Add**.
4. Enter a certificate name that contains at least 1 and no more than 32 characters.
5. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
6. In the **Certificate type** section, upload the client certificate, private key and CA bundle `.pem` files:
  - a. Select **Upload certificate** and then select **Continue**.
  - b. Upload client certificate, private key and CA bundle files (`.pem`).
    - Select **Client certificate details** to display the certificate metadata and certificate PEM.
    - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
  - c. Select **Create** to save the certificate in the Grid Manager.

The new certificates appear on the Client tab.

7. Configure the following settings on your external monitoring tool, such as Grafana.

- a. **Name:** Enter a name for the connection.

StorageGRID does not require this information, but you must provide a name to test the connection.

- b. **URL:** Enter the domain name or IP address for the Admin Node. Specify HTTPS and port 9091.

For example: `https://admin-node.example.com:9091`

- c. Enable **TLS Client Auth** and **With CA Cert**.
- d. Under TLS/SSL Auth Details, copy and paste:
  - The management interface CA certificate to **CA Cert**
  - The client certificate to **Client Cert**
  - The private key to **Client Key**
- e. **ServerName:** Enter the domain name of the Admin Node.

ServerName must match the domain name as it appears in the management interface certificate.

- f. Save and test the certificate and private key that you copied from StorageGRID or a local file.

You can now access the Prometheus metrics from StorageGRID with your external monitoring tool.

For information about the metrics, see the [instructions for monitoring StorageGRID](#).

### Generated certificate from Grid Manager

Use this procedure to add an administrator client certificate if a management interface certificate was not configured and you plan to add a client certificate for Prometheus that uses the generate certificate function in Grid Manager.

#### Steps

1. In the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.
2. Select **Add**.
3. Enter a certificate name that contains at least 1 and no more than 32 characters.
4. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
5. In the **Certificate type** section, select **Generate certificate**.
6. Specify the certificate information:
  - **Domain name:** One or more fully qualified domain names of the admin node to include in the certificate. Use an \* as a wildcard to represent multiple domain names.
  - **IP:** One or more admin node IP addresses to include in the certificate.
  - **Subject:** X.509 subject or distinguished name (DN) of the certificate owner.
7. Select **Generate**.
8. Select **Client certificate details** to display the certificate metadata and certificate PEM.



You will not be able to view the certificate private key after you close the dialog. Copy or download the key to a safe location.

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
- Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

- Select **Copy private key** to copy the certificate private key for pasting elsewhere.
- Select **Download private key** to save the private key as a file.

Specify the private key file name and download location.

9. Select **Create** to save the certificate in the Grid Manager.

The new certificate appears on the Client tab.

10. In the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates** and then select the **Global** tab.
11. Select **Management Interface certificate**.
12. Select **Use custom certificate**.
13. Upload the `certificate.pem` and `private_key.pem` files from the [client certificate details](#) step. There is no need to upload CA bundle.

- a. Select **Upload certificate** and then select **Continue**.
- b. Upload each certificate file (.pem).
- c. Select **Create** to save the certificate in the Grid Manager.

The new certificate appears on the Client tab.

14. Configure the following settings on your external monitoring tool, such as Grafana.

- a. **Name:** Enter a name for the connection.

StorageGRID does not require this information, but you must provide a name to test the connection.

- b. **URL:** Enter the domain name or IP address for the Admin Node. Specify HTTPS and port 9091.

For example: `https://admin-node.example.com:9091`

- c. Enable **TLS Client Auth** and **With CA Cert**.

- d. Under TLS/SSL Auth Details, copy and paste:

- The management interface client certificate to both **CA Cert** and **Client Cert**
- The private key to **Client Key**

- e. **ServerName:** Enter the domain name of the Admin Node.

ServerName must match the domain name as it appears in the management interface certificate.

- f. Save and test the certificate and private key that you copied from StorageGRID or a local file.

You can now access the Prometheus metrics from StorageGRID with your external monitoring tool.

For information about the metrics, see the [instructions for monitoring StorageGRID](#).

## Edit client certificates

You can edit an administrator client certificate to change its name, enable or disable Prometheus access, or upload a new certificate when the current one has expired.

### Steps

1. Select **CONFIGURATION > Security > Certificates** and then select the **Client** tab.

Certificate expiration dates and Prometheus access permissions are listed in the table. If a certificate will expire soon or is already expired, a message appears in the table and an alert is triggered.

2. Select the certificate you want to edit.
3. Select **Edit** and then select **Edit name and permission**
4. Enter a certificate name that contains at least 1 and no more than 32 characters.
5. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
6. Select **Continue** to save the certificate in the Grid Manager.

The updated certificate displays on the Client tab.

## Attach new client certificate

You can upload a new certificate when the current one has expired.

### Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.

Certificate expiration dates and Prometheus access permissions are listed in the table. If a certificate will expire soon or is already expired, a message appears in the table and an alert is triggered.

2. Select the certificate you want to edit.
3. Select **Edit** and then select an edit option.

### Upload certificate

Copy the certificate text to paste elsewhere.

1. Select **Upload certificate** and then select **Continue**.
2. Upload the client certificate name (.pem).

Select **Client certificate details** to display the certificate metadata and certificate PEM.

- Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension .pem.

For example: storagegrid\_certificate.pem

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.

3. Select **Create** to save the certificate in the Grid Manager.

The updated certificate displays on the Client tab.

### Generate certificate

Generate the certificate text to paste elsewhere.

1. Select **Generate certificate**.
2. Specify the certificate information:
  - **Domain name:** One or more fully qualified domain names to include in the certificate. Use an \* as a wildcard to represent multiple domain names.
  - **IP:** One or more IP addresses to include in the certificate.
  - **Subject:** X.509 subject or distinguished name (DN) of the certificate owner.
  - **Days valid:** Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Client certificate details** to display the certificate metadata and certificate PEM.



You will not be able to view the certificate private key after you close the dialog. Copy or download the key to a safe location.

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
- Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension .pem.

For example: storagegrid\_certificate.pem

- Select **Copy private key** to copy the certificate private key for pasting elsewhere.
- Select **Download private key** to save the private key as a file.

Specify the private key file name and download location.

5. Select **Create** to save the certificate in the Grid Manager.

The new certificate appears on the Client tab.

## Download or copy client certificates

You can download or copy a client certificate for use elsewhere.

### Steps

1. Select **CONFIGURATION > Security > Certificates** and then select the **Client** tab.
2. Select the certificate you want to copy or download.
3. Download or copy the certificate.

#### Download certificate file

Download the certificate .pem file.

1. Select **Download certificate**.
2. Specify the certificate file name and download location. Save the file with the extension .pem.

For example: `storagegrid_certificate.pem`

#### Copy certificate

Copy the certificate text to paste elsewhere.

1. Select **Copy certificate PEM**.
2. Paste the copied certificate into a text editor.
3. Save the text file with the extension .pem.

For example: `storagegrid_certificate.pem`

## Remove client certificates

If you no longer need an administrator client certificate, you can remove it.

### Steps

1. Select **CONFIGURATION > Security > Certificates** and then select the **Client** tab.
2. Select the certificate you want to remove.
3. Select **Delete** and then confirm.



To remove up to 10 certificates, select each certificate to remove on the Client tab and then select **Actions > Delete**.

After a certificate is removed, clients that used the certificate must specify a new client certificate to access the StorageGRID Prometheus database.

# 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 ( <b>CONFIGURATION &gt; Security &gt; Key management server</b> ) 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 <b>Node Encryption</b> enabled during installation. All data on the appliance is protected against physical loss or removal from the data center.   Managing encryption keys with a KMS is only supported for Storage Nodes and service 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.	<p>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.</p> <ul style="list-style-type: none"> <li>• <a href="#">SG6000 storage appliances</a></li> <li>• <a href="#">SG5700 storage appliances</a></li> <li>• <a href="#">SG5600 storage appliances</a></li> </ul>
Stored Object Encryption grid option	The <b>Stored Object Encryption</b> option can be enabled in the Grid Manager ( <b>CONFIGURATION &gt; System &gt; Grid options</b> ). When enabled, any new objects that are not encrypted at the bucket level or at the object level are encrypted during ingest.	<p>Newly ingested S3 and Swift object data.</p> <p>Existing stored objects are not encrypted. Object metadata and other sensitive data are not encrypted.</p> <ul style="list-style-type: none"> <li>• <a href="#">Configure stored object encryption</a></li> </ul>
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.	<p>Newly ingested S3 object data only.</p> <p>Encryption must be specified for the bucket. Existing bucket objects are not encrypted. Object metadata and other sensitive data are not encrypted.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>
S3 object server-side encryption (SSE)	You issue an S3 request to store an object and include the <code>x-amz-server-side-encryption</code> request header.	<p>Newly ingested S3 object data only.</p> <p>Encryption must be specified for the object. Object metadata and other sensitive data are not encrypted.</p> <p>StorageGRID manages the keys.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>

Encryption option	How it works	Applies to
S3 object server-side encryption with customer-provided keys (SSE-C)	<p>You issue an S3 request to store an object and include three request headers.</p> <ul style="list-style-type: none"> <li>• <code>x-amz-server-side-encryption-customer-algorithm</code></li> <li>• <code>x-amz-server-side-encryption-customer-key</code></li> <li>• <code>x-amz-server-side-encryption-customer-key-MD5</code></li> </ul>	<p>Newly ingested S3 object data only.</p> <p>Encryption must be specified for the object. Object metadata and other sensitive data are not encrypted.</p> <p>Keys are managed outside of StorageGRID.</p> <ul style="list-style-type: none"> <li>• <a href="#">Use S3</a></li> </ul>
External volume or datastore encryption	<p>You use an encryption method outside of StorageGRID to encrypt an entire volume or datastore, if your deployment platform supports it.</p>	<p>All object data, metadata, and system configuration data, assuming every volume or datastore is encrypted.</p> <p>An external encryption method provides tighter control over encryption algorithms and keys. Can be combined with the other methods listed.</p>
Object encryption outside of StorageGRID	<p>You use an encryption method outside of StorageGRID to encrypt object data and metadata before they are ingested into StorageGRID.</p>	<p>Object data and metadata only (system configuration data is not encrypted).</p> <p>An external encryption method provides tighter control over encryption algorithms and keys. Can be combined with the other methods listed.</p> <ul style="list-style-type: none"> <li>• <a href="#">Amazon Simple Storage Service - Developer Guide: Protecting data using client-side encryption</a></li> </ul>

## 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.

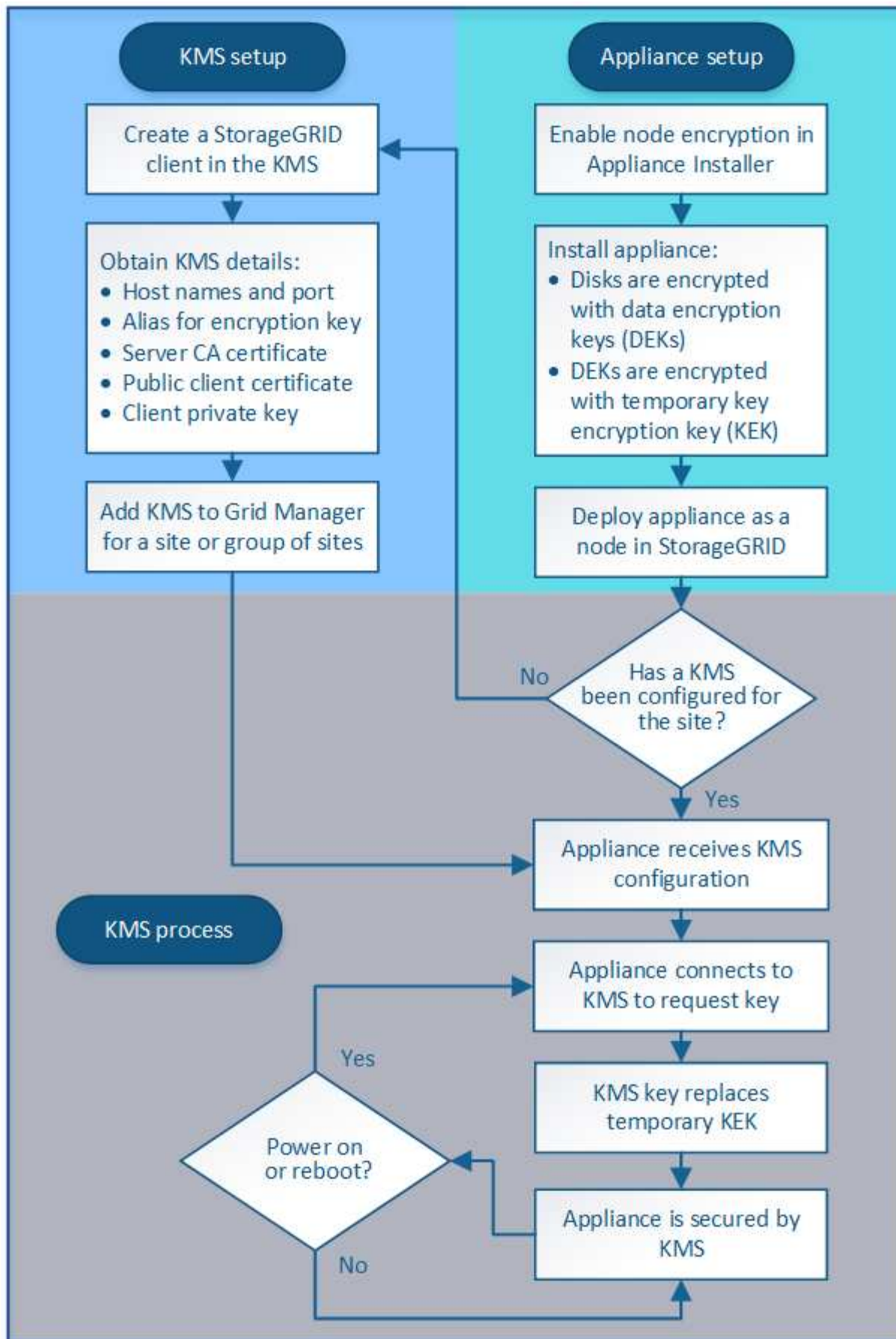
If only a small portion of your objects require encryption, consider controlling encryption at the bucket or

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.	<a href="#">Configure StorageGRID as a client in the KMS</a>
Obtain the required information for the StorageGRID client on the KMS.	<a href="#">Configure StorageGRID as a client in the KMS</a>
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.	<a href="#">Add a key management server (KMS)</a>

## 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.



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.



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.

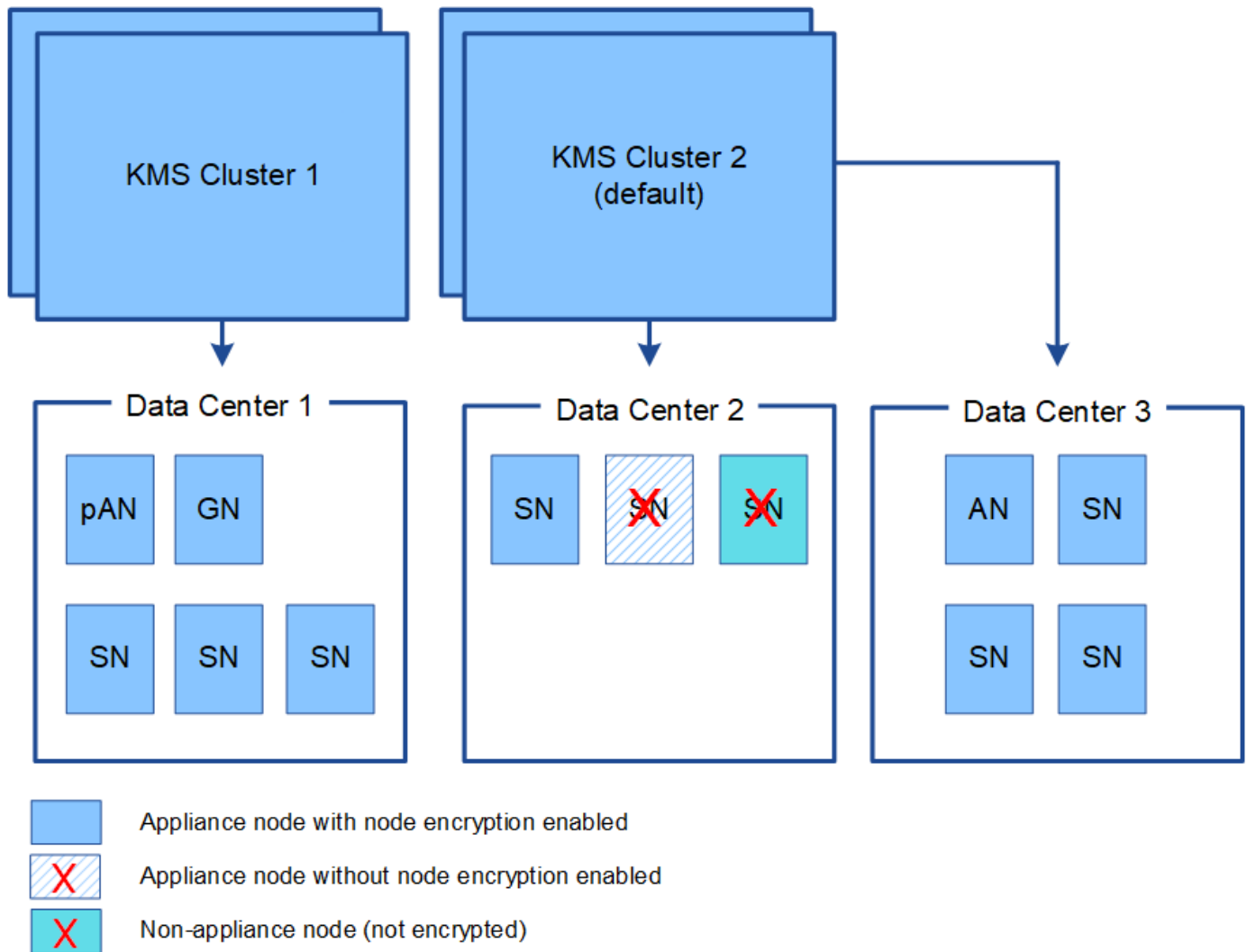
### How many key management servers do I need?

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.



### 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.



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](#)

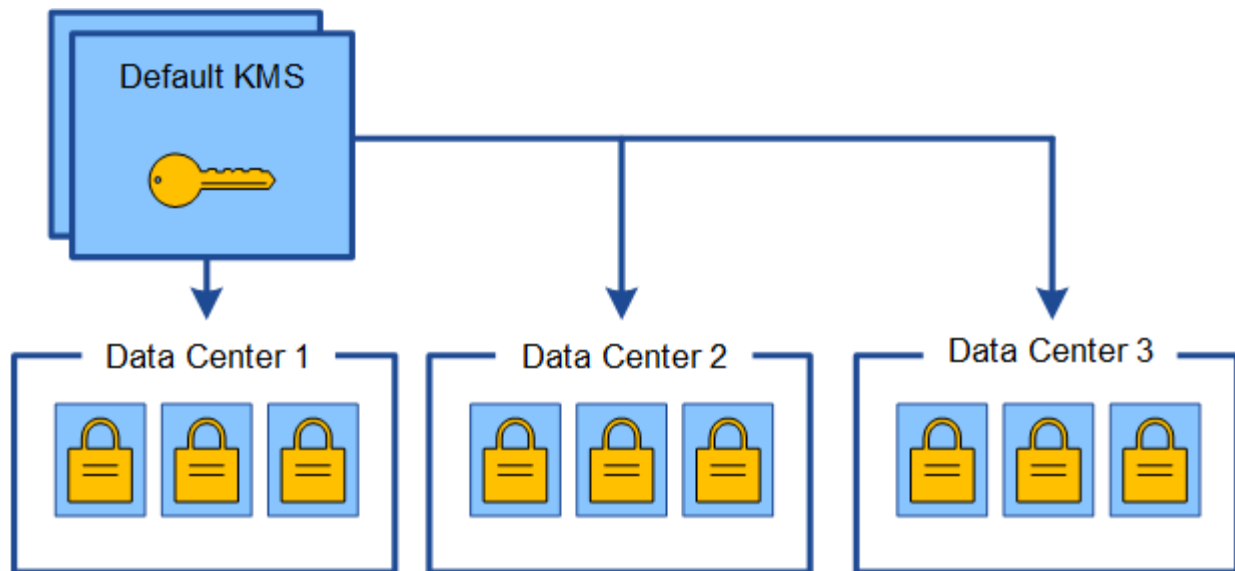
### Considerations for changing the KMS for a site

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.

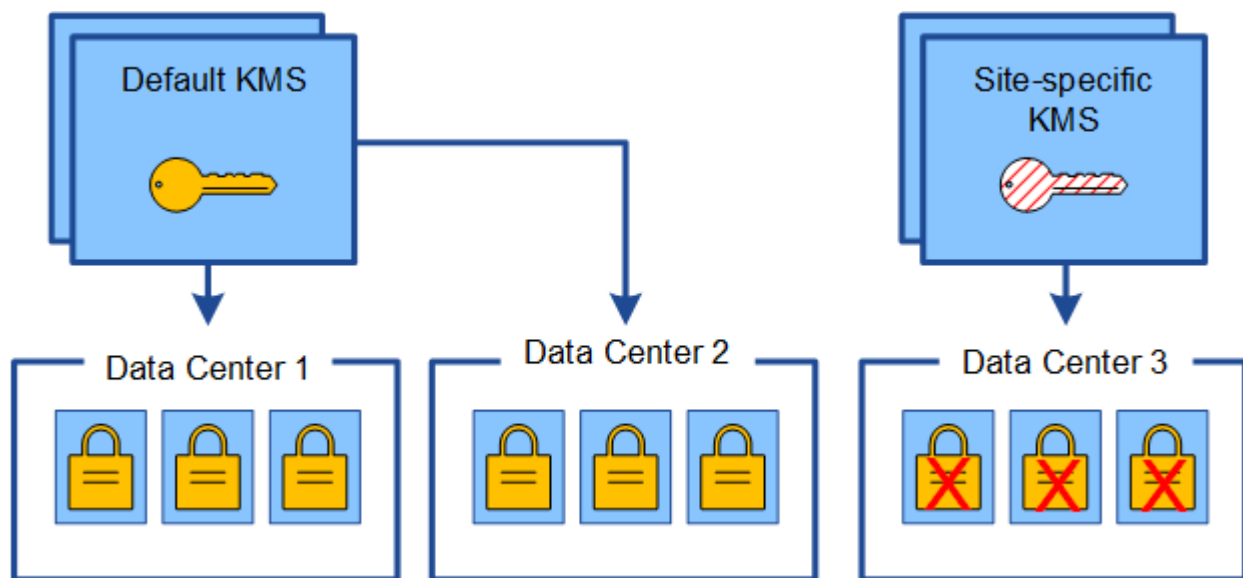
If you change the KMS used for a site, you must ensure that the previously encrypted appliance nodes at that site can be decrypted using the key stored on the new KMS. In some cases, you might need to copy the current version of the encryption key from the original KMS to the new KMS. You must ensure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

For example:

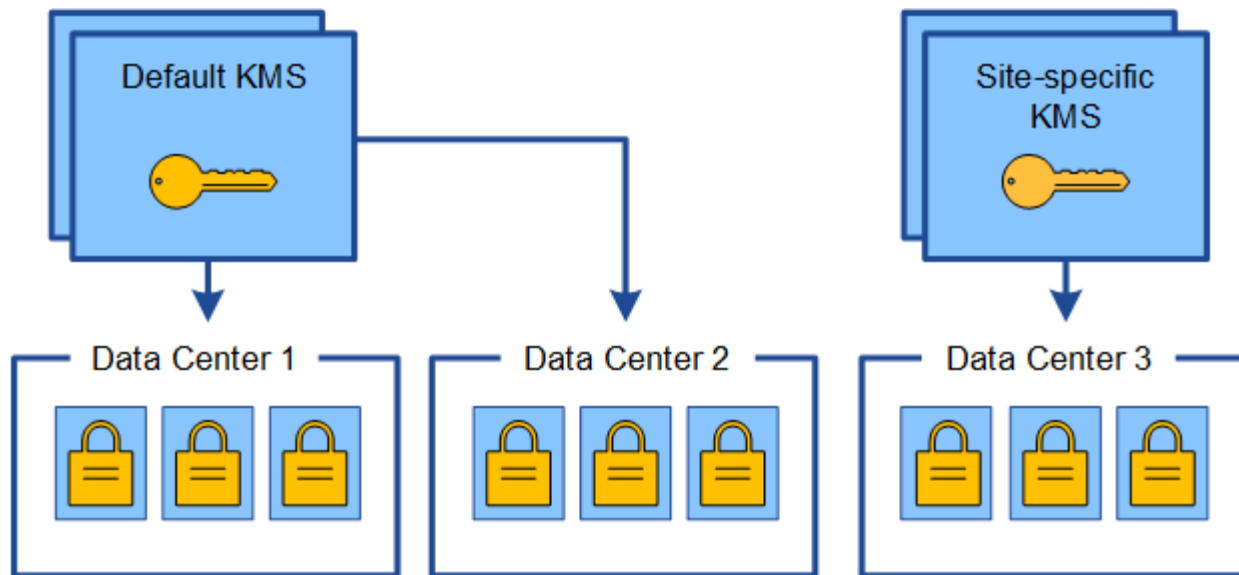
1. You initially configure a default KMS that applies to all sites that do not have a dedicated KMS.
2. When the KMS is saved, all appliance nodes that have the **Node Encryption** setting enabled connect to the KMS and request the encryption key. This key is used to encrypt the appliance nodes at all 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.	<p>Edit the site-specific KMS. In the <b>Manages keys for</b> field, select <b>Sites not managed by another KMS (default KMS)</b>. 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.</p> <p><a href="#">Edit a key management server (KMS)</a></p>
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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Using the Grid Manager, add the new KMS and select the site.</li> </ol> <p><a href="#">Add a key management server (KMS)</a></p>
You want the KMS for a site to use a different server.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Using the Grid Manager, edit the existing KMS configuration and enter the new host name or IP address.</li> </ol> <p><a href="#">Add a key management server (KMS)</a></p>

## 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.

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 ?
No key management servers have been configured. Select Create.				

2. Select **Create**.

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

## Add a Key Management Server



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	<input type="text"/>
Key Name	<input type="text"/>
Manages keys for	<input type="text" value="-- Choose One --"/>
Port	<input type="text" value="5696"/>
Hostname	<input type="text"/>



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	<p>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.</p> <ul style="list-style-type: none"> <li>• Select a site if this KMS will manage encryption keys for the appliance nodes at a specific site.</li> <li>• Select <b>Sites not managed by another KMS (default KMS)</b> 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.</li> </ul> <p><b>Note:</b> 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.</p>
Port	<p>The port the KMS server uses for Key Management Interoperability Protocol (KMIP) communications. Defaults to 5696, which is the KMIP standard port.</p>
Hostname	<p>The fully qualified domain name or IP address for the KMS.</p> <p><b>Note:</b> 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.</p>

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



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   k170vCA.pem

### Server Certificate 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



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.

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

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.

Cancel

Back

Force Save

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.

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.

Cancel

OK

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 <b>Sites not managed by another KMS (default KMS)</b> .

Field	Description
Hostname	<p>The fully qualified domain name or IP address of the KMS.</p> <p>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.</p> <p>For example: 10.10.10.10 and 10.10.10.11 or 10.10.10.10 and 2 others.</p> <p>To view all hostnames in a cluster, select a KMS and then select <b>Edit</b>.</p>
Certificate Status	<p>Current state of the server certificate, optional CA certificate, and the client certificate: valid, expired, nearing expiration, or unknown.</p> <p><b>Note:</b> 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.</p>

- 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.

- 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

- 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	<p>The descriptive name of the KMS used for the node.</p> <p>If no KMS is listed, select the Configuration Details tab to add a KMS.</p> <p><a href="#">Add a key management server (KMS)</a></p>
Key UID	<p>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.</p> <p>A dash (--) indicates the key UID is unknown, possibly because of a connection issue between the appliance node and the KMS.</p>
Status	<p>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.</p> <p><b>Note:</b> You must refresh your web browser to see the new values.</p>

- 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.

### 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 ?
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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	<p>The exact key alias for the StorageGRID client in the KMS. Must be between 1 and 255 characters.</p> <p>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.</p> <div>  <p>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.</p> <p><a href="#">Considerations and requirements for using a key management server</a></p> </div>
Manages keys for	<p>If you are editing a site-specific KMS and you do not already have a default KMS, optionally select <b>Sites not managed by another KMS (default KMS)</b>. 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.</p> <p><b>Note:</b> 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.</p>
Port	The port the KMS server uses for Key Management Interoperability Protocol (KMIP) communications. Defaults to 5696, which is the KMIP standard port.
Hostname	<p>The fully qualified domain name or IP address for the KMS.</p> <p><b>Note:</b> 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.</p>

- If you are configuring a KMS cluster, select the plus sign  to add a hostname for each server in the cluster.
- Select **Next**.

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

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

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

- 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.

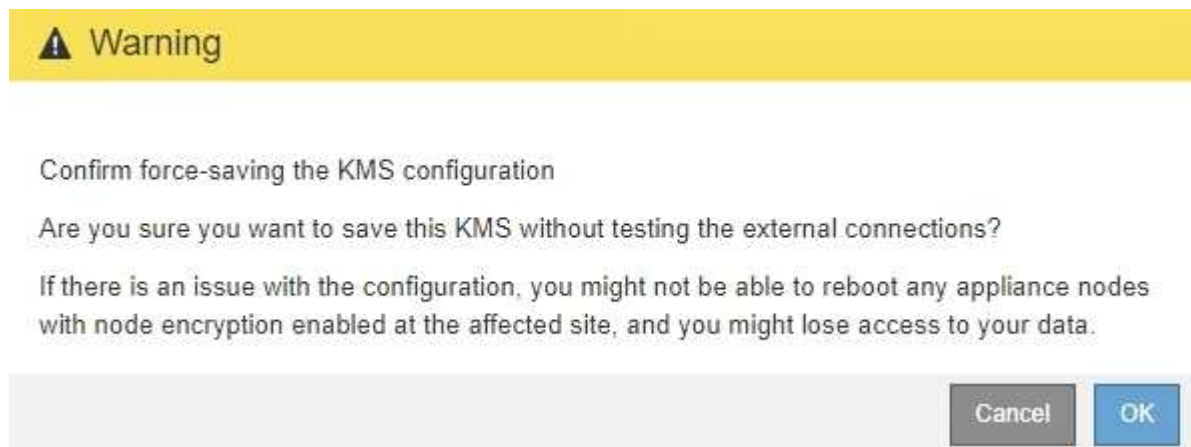
11. If you need to save the current configuration before resolving the connection errors, select **Force Save**.



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.



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 ?
<input checked="" type="radio"/> 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.

# Manage proxy settings

## Configure Storage proxy settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy between Storage Nodes and the external S3 endpoints. For example, you might need a non-transparent proxy to allow platform services messages to be sent to external endpoints, such as an endpoint on the internet.

### What you'll need

- You have specific access permissions.
- You are signed in to the Grid Manager using a [supported web browser](#).

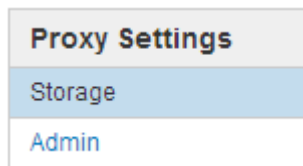
### About this task

You can configure the settings for a single Storage proxy.

### Steps

1. Select **CONFIGURATION** > **Security** > **Proxy settings**.

The Storage Proxy Settings page appears. By default, **Storage** is selected in the sidebar menu.



2. Select the **Enable Storage Proxy** check box.

The fields for configuring a Storage proxy appear.

#### Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☒ HTTP ☐ SOCKS5

Hostname

Port (optional)

3. Select the protocol for the non-transparent Storage proxy.
4. Enter the hostname or IP address of the proxy server.
5. Optionally, enter the port used to connect to the proxy server.

You can leave this field blank if you use the default port for the protocol: 80 for HTTP or 1080 for SOCKS5.

6. Select **Save**.

After the Storage proxy is saved, new endpoints for platform services or Cloud Storage Pools can be configured and tested.



Proxy changes can take up to 10 minutes to take effect.

7. Check the settings of your proxy server to ensure that platform service-related messages from StorageGRID will not be blocked.

### After you finish

If you need to disable a Storage proxy, deselect the **Enable Storage Proxy** check box, and select **Save**.

### Related information

- [Network and ports for platform services](#)
- [Manage objects with ILM](#)

## Configure Admin proxy settings

If you send AutoSupport messages using HTTP or HTTPS (see [Configure AutoSupport](#)), you can configure a non-transparent proxy server between Admin Nodes and technical support (AutoSupport).

### What you'll need

- You have specific access permissions.
- You are signed in to the Grid Manager using a [supported web browser](#).

### About this task

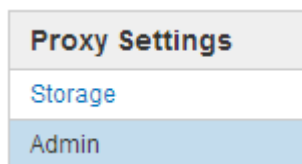
You can configure the settings for a single Admin proxy.

### Steps

1. Select **CONFIGURATION** > **Security** > **Proxy settings**.

The Admin Proxy Settings page appears. By default, **Storage** is selected in the sidebar menu.

2. From the sidebar menu, select **Admin**.



3. Select the **Enable Admin Proxy** check box.

## Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy ☒

Hostname

Port

Username (optional)

Password (optional)

4. Enter the hostname or IP address of the proxy server.

5. Enter the port used to connect to the proxy server.

6. Optionally, enter the proxy username.

Leave this field blank if your proxy server does not require a username.

7. Optionally, enter the proxy password.

Leave this field blank if your proxy server does not require a password.

8. Select **Save**.

After the Admin proxy is saved, the proxy server between Admin Nodes and technical support is configured.



Proxy changes can take up to 10 minutes to take effect.

9. If you need to disable the proxy, deselect the **Enable Admin Proxy** check box, and select **Save**.

## Manage untrusted Client Networks

### Manage untrusted Client Networks: Overview

If you are using a Client Network, you can help secure StorageGRID from hostile attacks by accepting inbound client traffic only on explicitly configured endpoints.

By default, the Client Network on each grid node is *trusted*. That is, by default, StorageGRID trusts inbound connections to each grid node on all available external ports (see the information about external communications in the [Networking guidelines](#)).

You can reduce the threat of hostile attacks on your StorageGRID system by specifying that the Client Network on each node be *untrusted*. If a node's Client Network is untrusted, the node only accepts inbound connections on ports explicitly configured as load balancer endpoints. See [Configure load balancer endpoints](#).

### Example 1: Gateway Node only accepts HTTPS S3 requests

Suppose you want a Gateway Node to refuse all inbound traffic on the Client Network except for HTTPS S3 requests. You would perform these general steps:

1. From the Load Balancer Endpoints page, configure a load balancer endpoint for S3 over HTTPS on port 443.
2. From the Untrusted Client Networks page, specify that the Client Network on the Gateway Node is untrusted.

After you save your configuration, all inbound traffic on the Gateway Node's Client Network is dropped except for HTTPS S3 requests on port 443 and ICMP echo (ping) requests.

### Example 2: Storage Node sends S3 platform services requests

Suppose you want to enable outbound S3 platform service traffic from a Storage Node, but you want to prevent any inbound connections to that Storage Node on the Client Network. You would perform this general step:

- From the Untrusted Client Networks page, indicate that the Client Network on the Storage Node is untrusted.

After you save your configuration, the Storage Node no longer accepts any incoming traffic on the Client Network, but it continues to allow outbound requests to Amazon Web Services.

## Specify node's Client Network is untrusted

If you are using a Client Network, you can specify whether each node's Client Network is trusted or untrusted. You can also specify the default setting for new nodes added in an expansion.

### What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the Root access permission.
- If you want an Admin Node or Gateway Node to accept inbound traffic only on explicitly configured endpoints, you have defined the load balancer endpoints.



Existing client connections might fail if load balancer endpoints have not been configured.

### Steps

1. Select **CONFIGURATION > Security > Untrusted Client Networks**.

The Untrusted Client Networks page lists all nodes in your StorageGRID system. The Unavailable Reason column includes an entry if the Client Network on the node must be trusted.



## Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network    ☒ Trusted  
Default    ☐ Untrusted

### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

- In the **Set New Node Default** section, specify what the default setting should be when new nodes are added to the grid in an expansion procedure.
  - Trusted:** When a node is added in an expansion, its Client Network is trusted.
  - Untrusted:** When a node is added in an expansion, its Client Network is untrusted. As required, you can return to this page to change the setting for a specific new node.



This setting does not affect the existing nodes in your StorageGRID system.

- In the **Select Untrusted Client Network Nodes** section, select the nodes that should allow client connections only on explicitly configured load balancer endpoints.

You can select or unselect the check box in the title to select or unselect all nodes.

- Select **Save**.

The new firewall rules are immediately added and enforced. Existing client connections might fail if load balancer endpoints have not been configured.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.