NetApp StorageGRID and Entrust KeyControl

Integration Guide

2024-07-22

Table of Contents

Chapter 1. Introduction

NetApp StorageGRID provides several ways to encrypt your data at rest including the use of external key management servers. Entrust KeyControl is a supported key management solution for StorageGRID node encryption. KeyControl provides a highly available decentralized vault-based solution that is compliant with the Key Management Interoperability Protocol (KMIP). This makes KeyControl an excellent option for StorageGRID.

1.1. Product configuration

NetApp StorageGRID and Entrust KeyControl were tested with the following configuration:

Product	Version
NetApp StorageGRID	11.8
Entrust KeyControl	10.2

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- NetApp StorageGRID documentation
- Entrust KeyControl Online Documentation Set

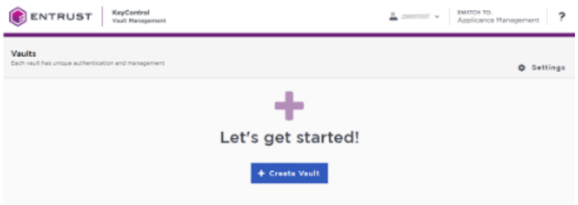
Chapter 2. Procedures

The steps in this section describe a single-site StorageGRID solution containing a mix of virtual appliances and a physical appliance. Only the physical appliance will be encrypted with a key from two KeyControl servers.

2.1. Deploy KeyControl and create a vault

1. Deploy KeyControl deployment and install the clustered KeyControl server.
2. Create a new vault.

   In KeyControl, select **Create Vault**.

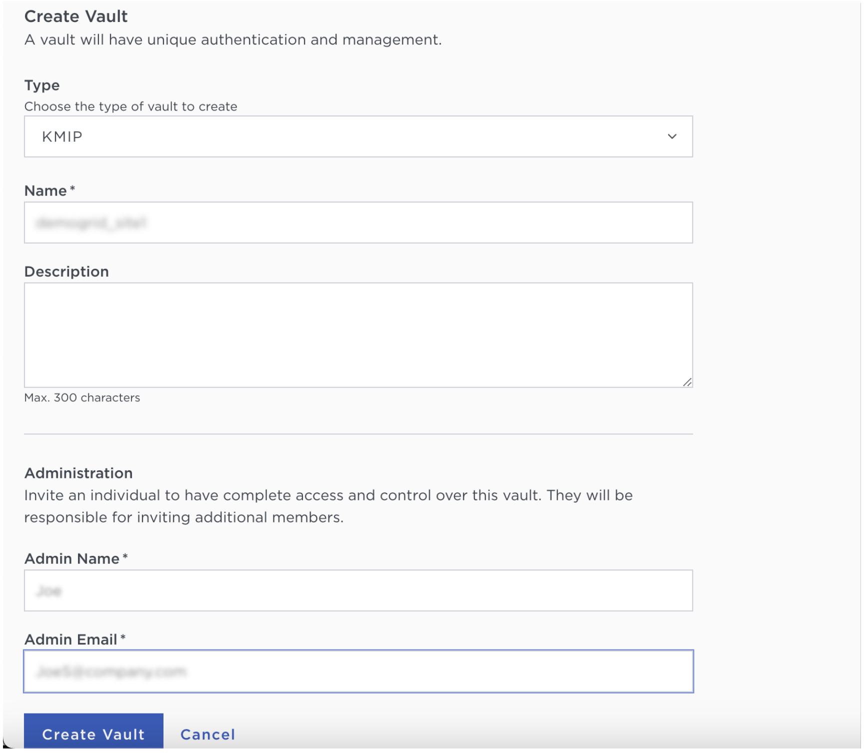


Vaults

Each vault has unique authentication and management

Let's get started!

3. Create a `KMIP` vault type and fill in the details for the vault.



Create Vault

A vault will have unique authentication and management.

Type

Choose the type of vault to create

KMIP

Name *

[redacted]

Description

Max. 300 characters

Administration

Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.

Admin Name *

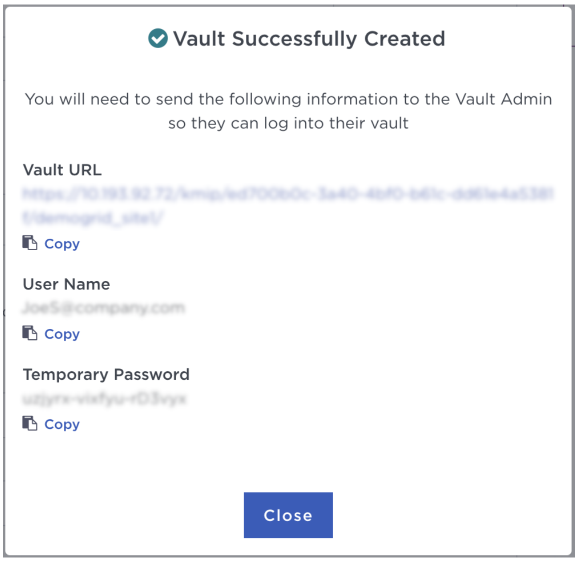
[redacted]

Admin Email *

[redacted]

   The admin email address will be the login name for the vault.

4. When the vault has been created, make a copy of the vault information: the link to the vault URL, the user name, and the randomly generated temporary password.



Vault Successfully Created

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL

[redacted]

User Name

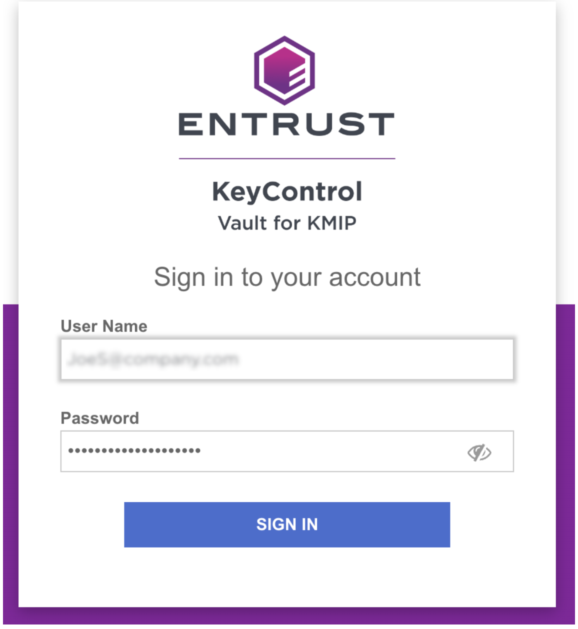
[redacted]

Temporary Password

[redacted]

2.2. Create a client certificate

1. Launch the vault from the URL and sign in with the new credentials. You will be prompted to set a new password and log in with the new password.

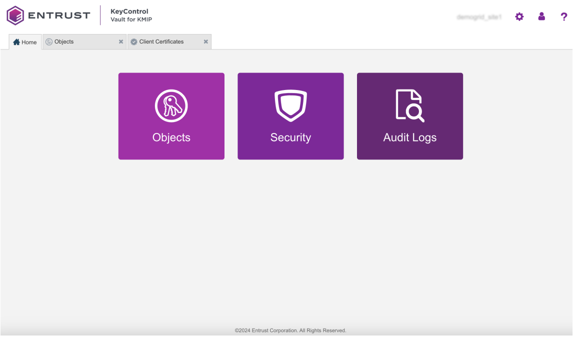


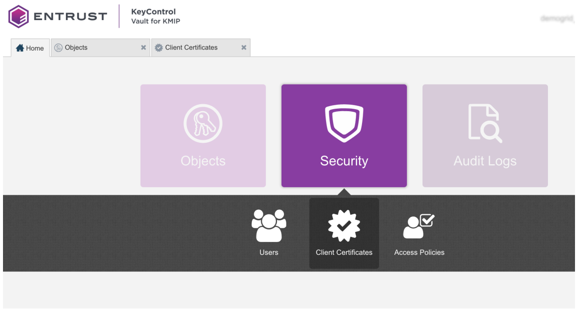
Sign in to your account

User Name: [redacted]

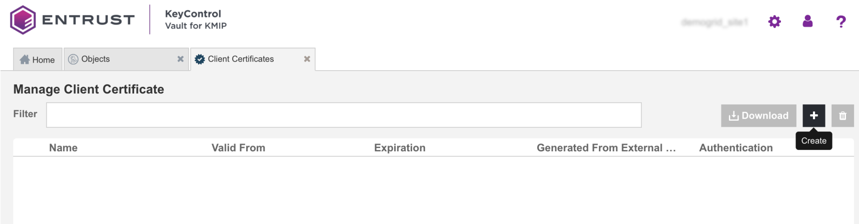
Password: ••••••••••••••••••••

2. When you logged in with the new password, select the large **Security** tile in the middle.
3. On **Client Certificates**, create the certificate bundle to authenticate StorageGRID to the KMS.





4. In **Client certificate**, select the plus sign (**+**) to create a new certificate.



Manage Client Certificate

Filter

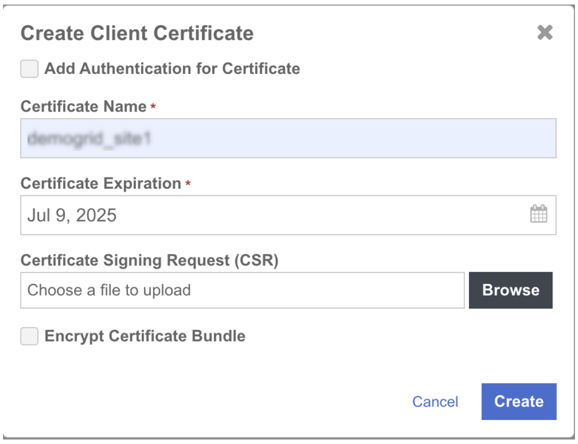
Name	Valid From	Expiration	Generated From External ...	Authentication

5. Provide a name and an expiration date for the certificate.

   This integration does not have a CSR to upload so we clear the checkbox for authentication and encryption.

   Select **Create**.

   The new certificate is generated and it appears in the **Manage Client Certificate** list.



Create Client Certificate

□ Add Authentication for Certificate

Certificate Name *

[redacted]

Certificate Expiration *

Jul 9, 2025

Certificate Signing Request (CSR)

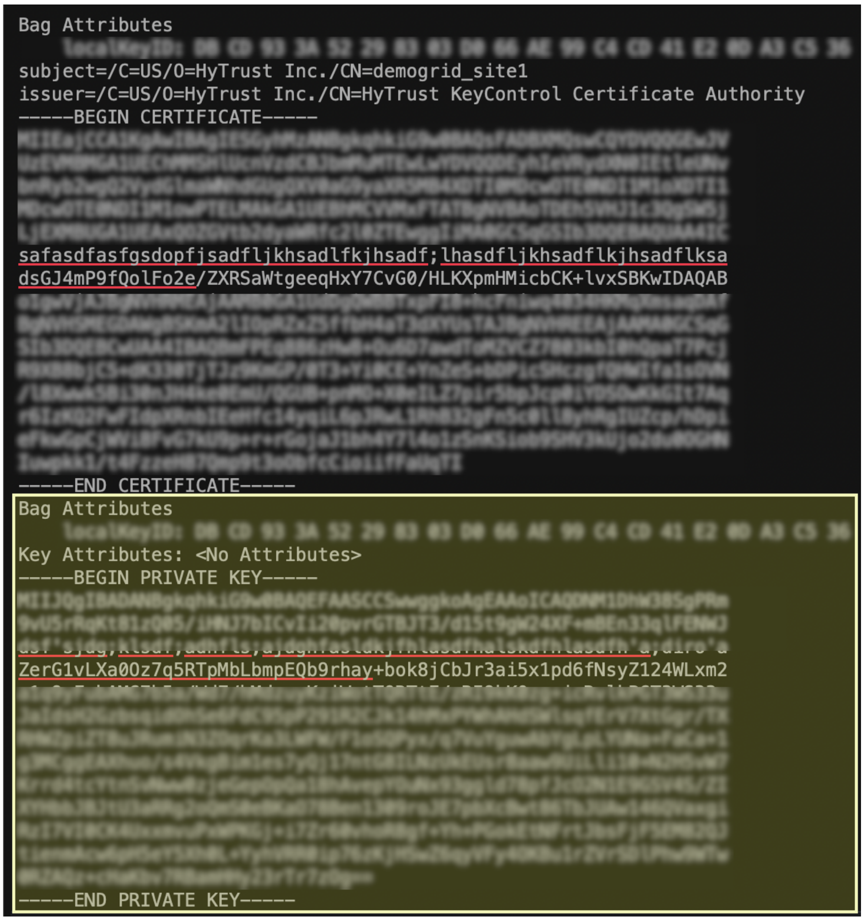
Choose a file to upload

□ Encrypt Certificate Bundle

6. Select the new certificate, download and unzip it.

   There are two `.pem` files: `cacert.pem` and `certificate_name.pem`.

   The named certificate file is a combined certificate and key that will need to be separated out into individual files with the Key text (highlighted in yellow) as a new file named `certificate_name.key`.



```
Bag Attributes
[redacted]
subject=/C=US/O=HyTrust Inc./CN=demogrid_site1
issuer=/C=US/O=HyTrust Inc./CN=HyTrust KeyControl Certificate Authority
-----BEGIN CERTIFICATE-----
[redacted]
safasdfasfgsdopfjsadfljkhsadlfkjhsadf;lhasdfljkhsadflkjhsadflksa
dsGJ4mP9fQolFo2e/ZXRSaWtgeeqHxY7CvG0/HLKXpmHMicbCK+lvxSBKwIDAQAB
[redacted]
-----END CERTIFICATE-----
Bag Attributes
[redacted]
Key Attributes: <No Attributes>
-----BEGIN PRIVATE KEY-----
[redacted]
ZerG1vLXa0Oz7q5RTpMbLbmpEQb9rhay+bok8jCbJr3ai5x1pd6fNsyZ124WLxm2
[redacted]
-----END PRIVATE KEY-----
```

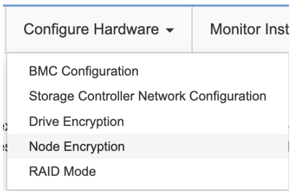
2.3. Configure StorageGRID

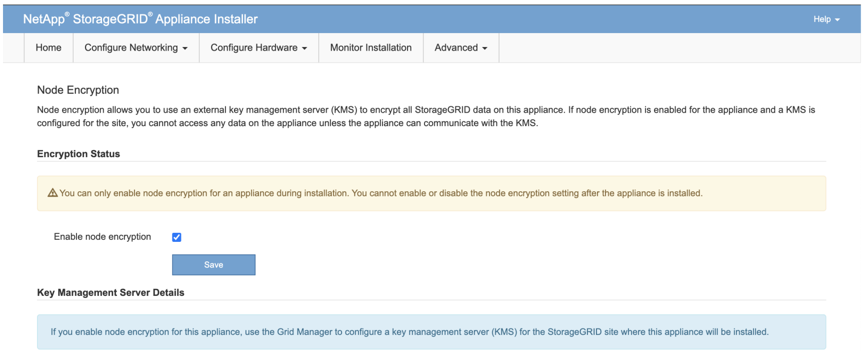
Appliances can only use node encryption with an external KMS if it is configured when the appliance is installed.

1. From inside the installer UI, select **Configure Hardware > Node Encryption**, select the checkbox to enable node encryption, then select **Save**.

   Repeat this step for all nodes to be encrypted.

   The nodes are now ready to be joined to the StorageGRID solution.





Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

⚠ You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

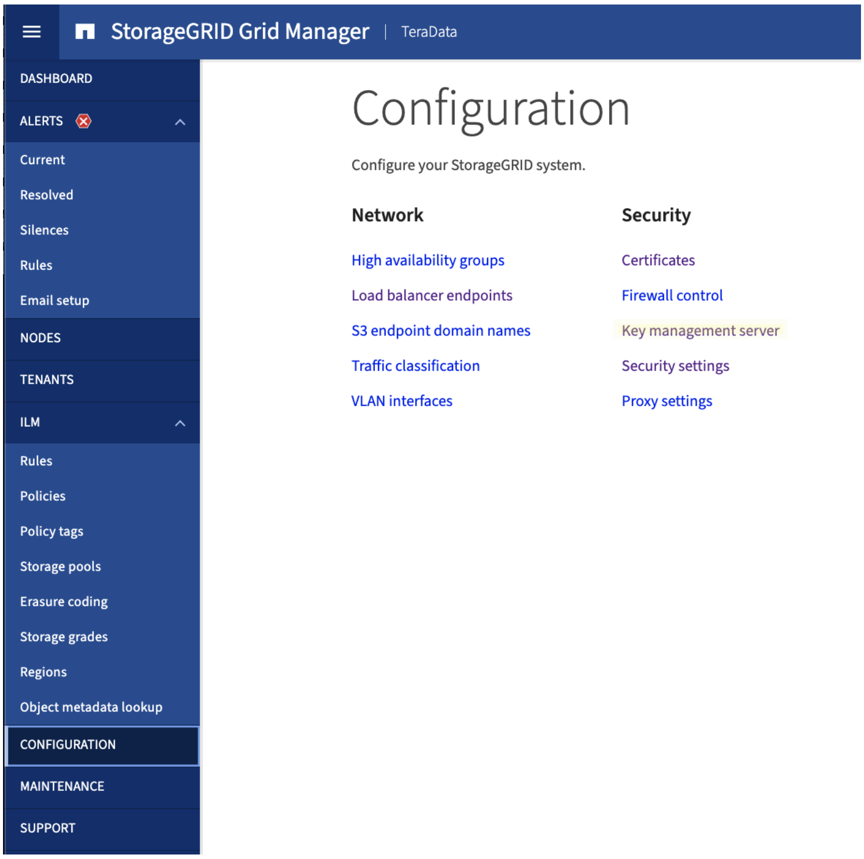
Enable node encryption ☑

Save

Key Management Server Details

If you enable node encryption for this appliance, use the Grid Manager to configure a key management server (KMS) for the StorageGRID site where this appliance will be installed.

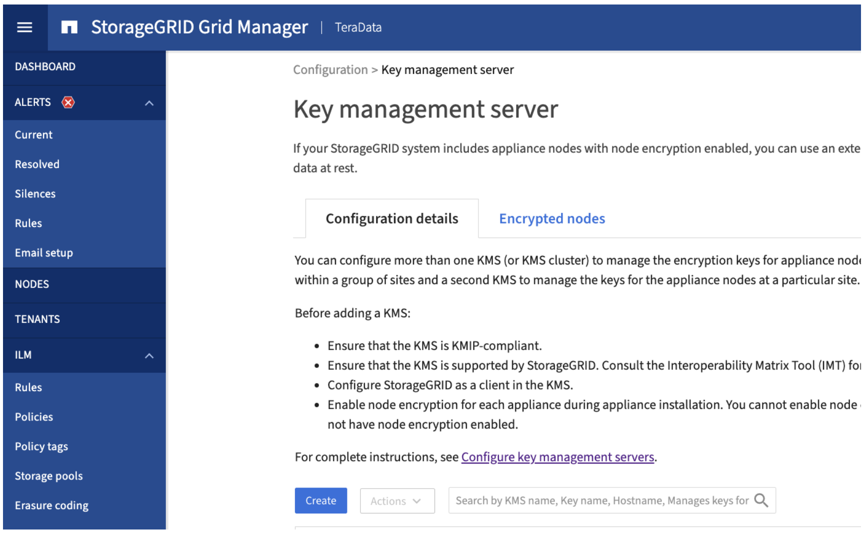
2. Install the node or nodes and join them to the grid.
3. Configure StorageGRID to use the KeyControl cluster for a KMS. In the StorageGRID management UI, select **Configuration> Security> Key management server**.



Configuration

Configure your StorageGRID system.

4. Select **Create** add the new KeyControl KMS.



StorageGRID Grid Manager | TeraData

Configuration > Key management server

Key management server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an exte
data at rest.

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

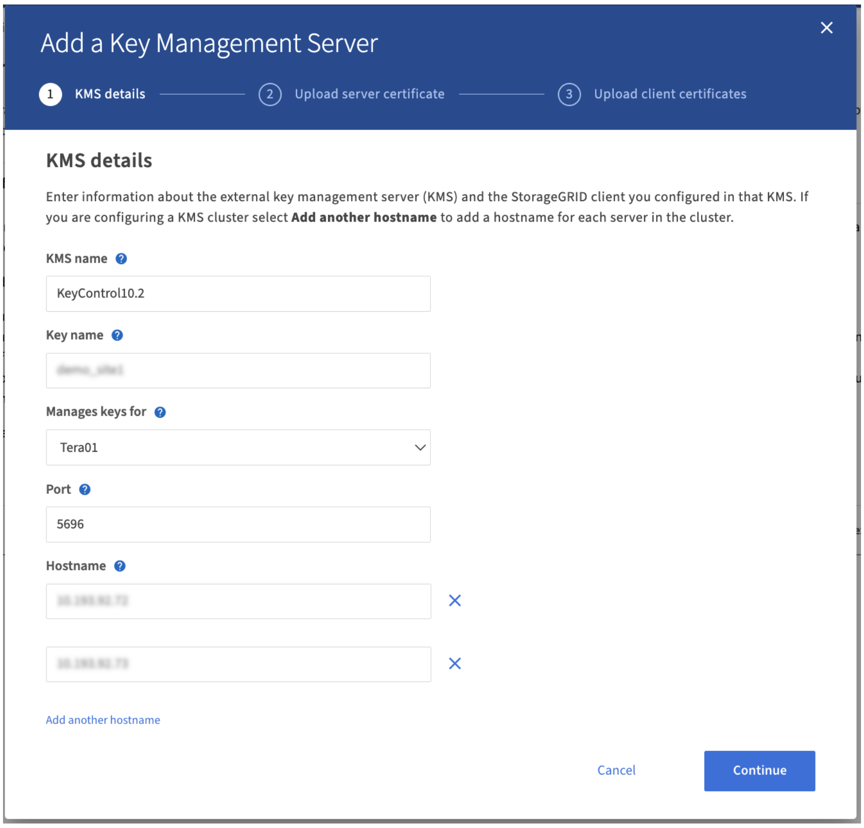
Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Ensure that the KMS is supported by StorageGRID. Consult the Interoperability Matrix Tool (IMT) fo
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node
  not have node encryption enabled.

For complete instructions, see Configure key management servers.

5. Ender the details for the new KMS configuration.

   Provide a name to identify the KMS, an encryption Key name (if one exists already in the KeyControl Vault that you wish to use, or this will be the name of the new key created by this process), what site should be managed by this KMS or all sites not managed by another configured KMS, the port should remain the default, and the hostnames or IP addresses of the KeyControl servers in the cluster.



Add a Key Management Server

KMS details

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 **Add another hostname** to add a hostname for each server in the cluster.

KMS name: KeyControl10.2

Key name: [redacted]

Manages keys for: Tera01

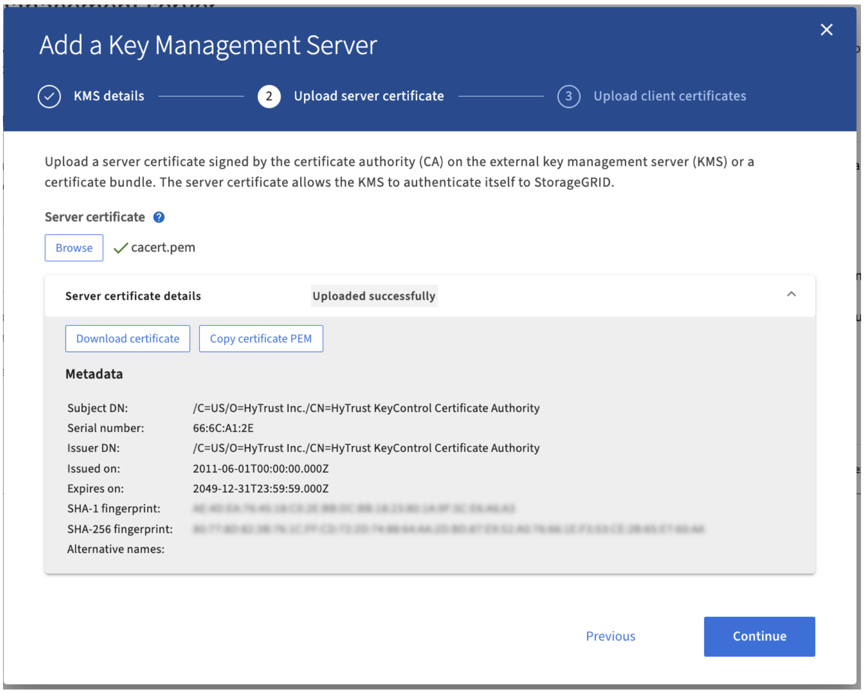
Port: 5696

Hostname: [redacted]

[redacted]

6. Select **Continue** to get to the next page to upload the server certificate.

This is the `cacert.pem` file that was provided by the KeyControl client certificate creation.


Add a Key Management Server
×
KMS details
2 Upload server certificate
3 Upload client certificates

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

Server certificate

Browse ✓ cacert.pem

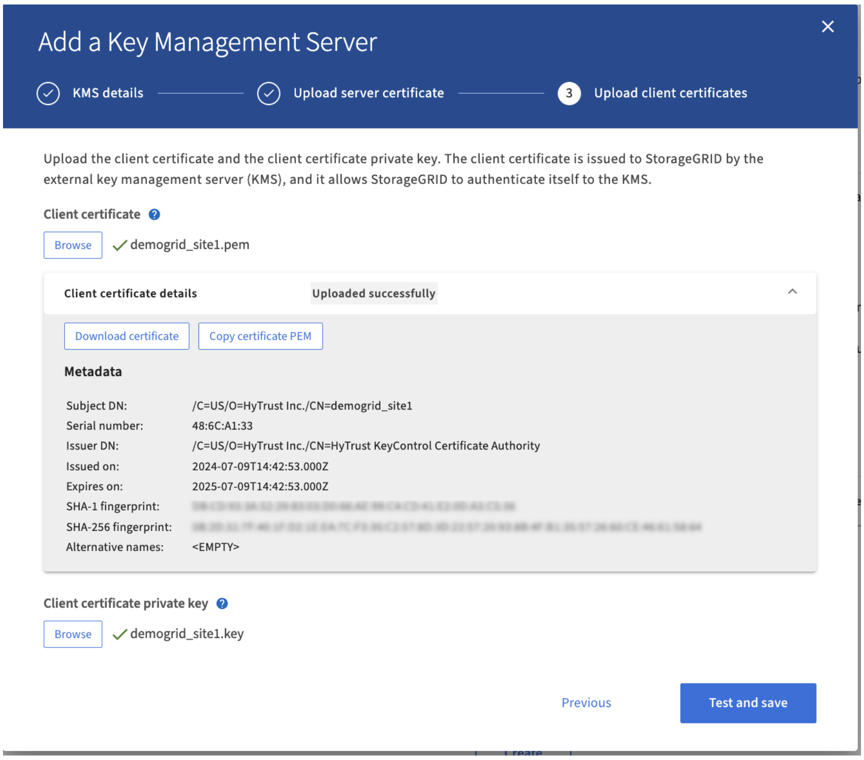
Server certificate details Uploaded successfully

Download certificate
Copy certificate PEM

Metadata

Subject DN: /C=US/O=HyTrust Inc./CN=HyTrust KeyControl Certificate Authority
Serial number: 66:6C:A1:2E
Issuer DN: /C=US/O=HyTrust Inc./CN=HyTrust KeyControl Certificate Authority
Issued on: 2011-06-01T00:00:00.000Z
Expires on: 2049-12-31T23:59:59.000Z
SHA-1 fingerprint: [redacted]
SHA-256 fingerprint: [redacted]
Alternative names:

7. Select **Continue** to upload the client certificate and key files.


Add a Key Management Server
×
KMS details
Upload server certificate
3 Upload client certificates

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

Client certificate

Browse ✓ demogrid_site1.pem

Client certificate details Uploaded successfully

Download certificate
Copy certificate PEM

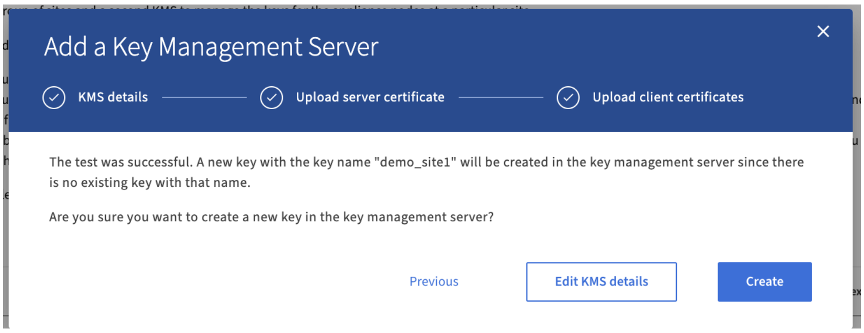
Metadata

Subject DN: /C=US/O=HyTrust Inc./CN=demogrid_site1
Serial number: 48:6C:A1:33
Issuer DN: /C=US/O=HyTrust Inc./CN=HyTrust KeyControl Certificate Authority
Issued on: 2024-07-09T14:42:53.000Z
Expires on: 2025-07-09T14:42:53.000Z
SHA-1 fingerprint: [redacted]
SHA-256 fingerprint: [redacted]
Alternative names: <EMPTY>

Client certificate private key

Browse ✓ demogrid_site1.key

8. Select **Test and save**.
9. If all went well the final dialog informs you that no key exists in the vault and a new key will be created.



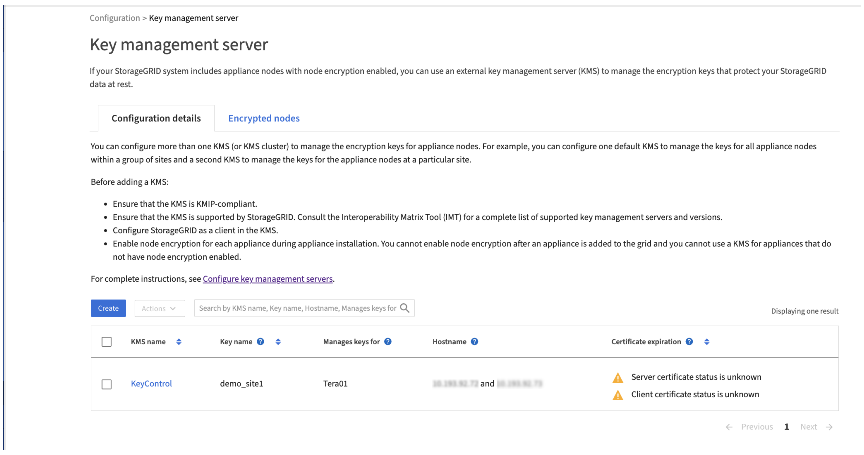
Add a Key Management Server

The test was successful. A new key with the key name "demo_site1" will be created in the key management server since there is no existing key with that name.

Are you sure you want to create a new key in the key management server?

10. When the key has been created, you can see the new KMS in the list with a certificate status unknown.

    After a few minutes this will update to show the certificates are valid.



Configuration > Key management server

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 data at rest.

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.

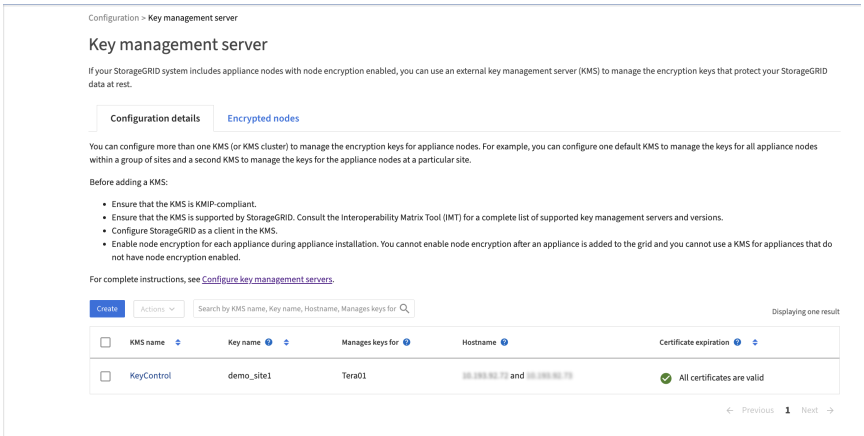
Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Ensure that the KMS is supported by StorageGRID. Consult the Interoperability Matrix Tool (IMT) for a complete list of supported key management servers and versions.
- 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 Configure key management servers.

Displaying one result

□	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
□	KeyControl	demo_site1	Tera01	[redacted] and [redacted]	⚠ Server certificate status is unknown ⚠ Client certificate status is unknown



Configuration > Key management server

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 data at rest.

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.
- Ensure that the KMS is supported by StorageGRID. Consult the Interoperability Matrix Tool (IMT) for a complete list of supported key management servers and versions.
- 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.

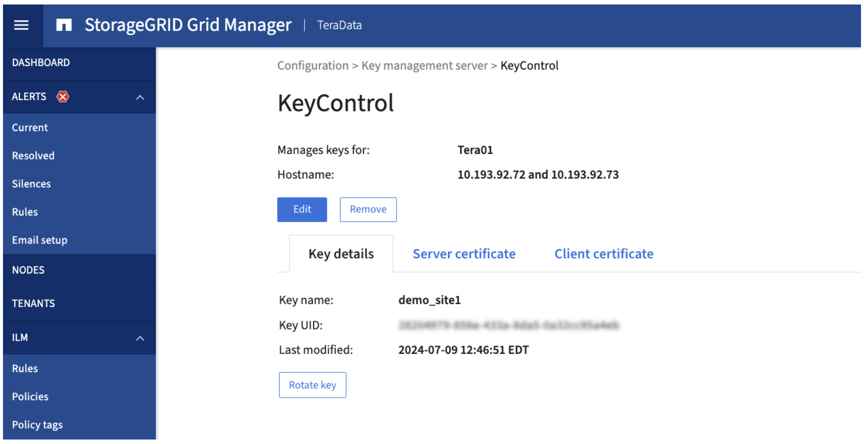
For complete instructions, see Configure key management servers.

Displaying one result

□	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
□	KeyControl	demo_site1	Tera01	[redacted] and [redacted]	✓ All certificates are valid

11. Select the KMS name to bring up the information on the KMS.

    This is also where you can choose to rotate the keys.



Configuration > Key management server > KeyControl

KeyControl

Manages keys for: Tera01

Hostname: 10.193.92.72 and 10.193.92.73

Edit Remove

Key details | Server certificate | Client certificate

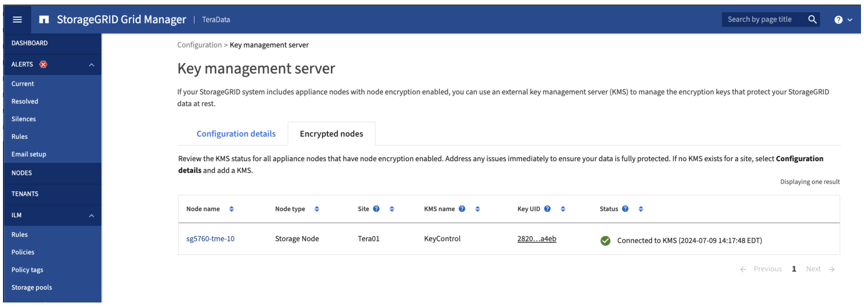
Key name: demo_site1

Key UID: [redacted]

Last modified: 2024-07-09 12:46:51 EDT

Rotate key

12. Select **Encrypted nodes** and verify which nodes are encrypted and which keys are used.



Configuration > Key management server

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 data at rest.

Configuration details | Encrypted nodes

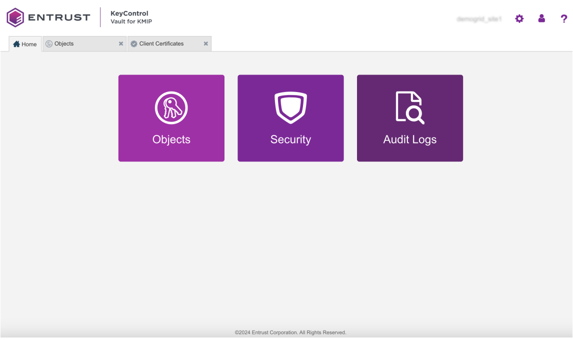
Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select **Configuration details** and add a KMS.

Displaying one result

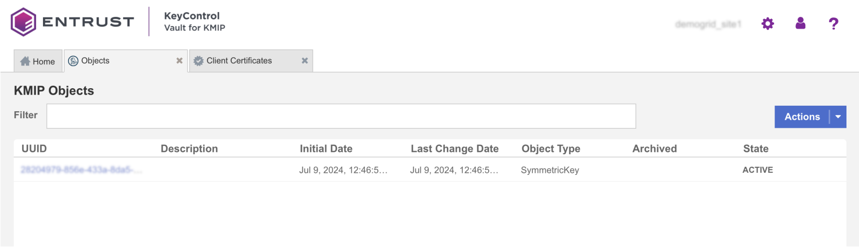
Node name	Node type	Site	KMS name	Key UID	Status
sg5760-tme-10	Storage Node	Tera01	KeyControl	2820…a4eb	✓ Connected to KMS (2024-07-09 14:17:48 EDT)

← Previous 1 Next →

13. Open KeyControl and in **Vault Objects** and check the keys in the vault and compare them to the StorageGRID keys that are in use.



©2024 Entrust Corporation. All Rights Reserved.



KMIP Objects

Filter

UUID	Description	Initial Date	Last Change Date	Object Type	Archived	State
[redacted]		Jul 9, 2024, 12:46:5…	Jul 9, 2024, 12:46:5…	SymmetricKey		ACTIVE

Chapter 3. Additional resources and related products

3.1. nShield Connect

3.2. nShield as a Service

3.3. KeyControl

3.4. Entrust products

3.5. nShield product documentation