NetApp

Administering a StorageGRID system

StorageGRID

NetApp
October 03, 2025

Table of Contents

Administering a StorageGRID system

Use these instructions to configure and administer a StorageGRID system.

These instructions describe how to use the Grid Manager to set up groups and users, create tenant accounts to allow S3 and Swift client applications to store and retrieve objects, configure and manage StorageGRID networks, configure AutoSupport, manage node settings, and more.

> ⓘ   The instructions for managing objects with information lifecycle management (ILM) rules and policies have been moved to Manage objects with ILM.

These instructions are for technical personnel who will be configuring, administering, and supporting a StorageGRID system after it has been installed.

What you'll need

- You have a general understanding of the StorageGRID system.
- You have fairly detailed knowledge of Linux command shells, networking, and server hardware setup and configuration.

Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

Signing in to the Grid Manager

You access the Grid Manager sign-in page by entering the fully qualified domain name (FQDN) or IP address of an Admin Node into the address bar of a supported web browser.

What you'll need

- You must have your login credentials.

- You must have the URL for the Grid Manager.

- You must be using a supported web browser.

- Cookies must be enabled in your web browser.

- You must have specific access permissions.

About this task

Each StorageGRID system includes one primary Admin Node and any number of non-primary Admin Nodes. You can sign in to the Grid Manager on any Admin Node to manage the StorageGRID system. However, the Admin Nodes are not exactly the same:

- Alarm acknowledgments (legacy system) made on one Admin Node are not copied to other Admin Nodes. For this reason, the information displayed for alarms might not look the same on each Admin Node.

- Some maintenance procedures can only be performed from the primary Admin Node.

If Admin Nodes are included in a high availability (HA) group, you connect using the virtual IP address of the HA group or a fully qualified domain name that maps to the virtual IP address. The primary Admin Node should be selected as the group's preferred Master, so that when you access the Grid Manager, you access it on the primary Admin Node unless the primary Admin Node is not available.

Steps

1. Launch a supported web browser.

2. In the browser's address bar, enter the URL for the Grid Manager:

   `https://FQDN_or_Admin_Node_IP/`

   where `FQDN_or_Admin_Node_IP` is a fully qualified domain name or the IP address of an Admin Node or the virtual IP address of an HA group of Admin Nodes.

   If you must access the Grid Manager on a port other than the standard port for HTTPS (443), enter the following, where `FQDN_or_Admin_Node_IP` is a fully qualified domain name or IP address, and port is the port number:

   `https://FQDN_or_Admin_Node_IP:port/`

3. If you are prompted with a security alert, install the certificate using the browser's installation wizard.

4. Sign in to the Grid Manager:

   - If single sign-on (SSO) is not being used for your StorageGRID system:

     i. Enter your username and password for the Grid Manager.

     ii. Click **Sign In**.

- If SSO is enabled for your StorageGRID system and this is the first time you have accessed the URL on this browser:

    i. Click **Sign in**. You can leave the Account ID field blank.
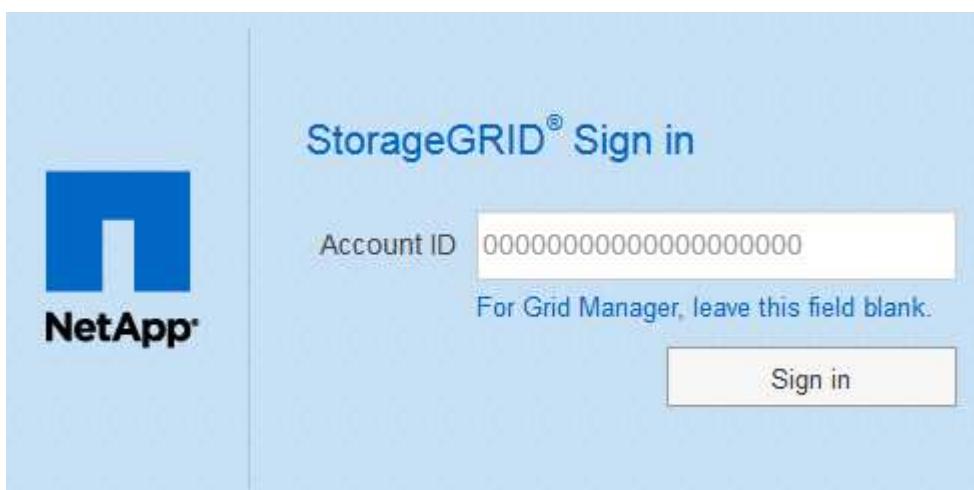
    ii. Enter your standard SSO credentials on your organization's SSO sign-in page. For example:
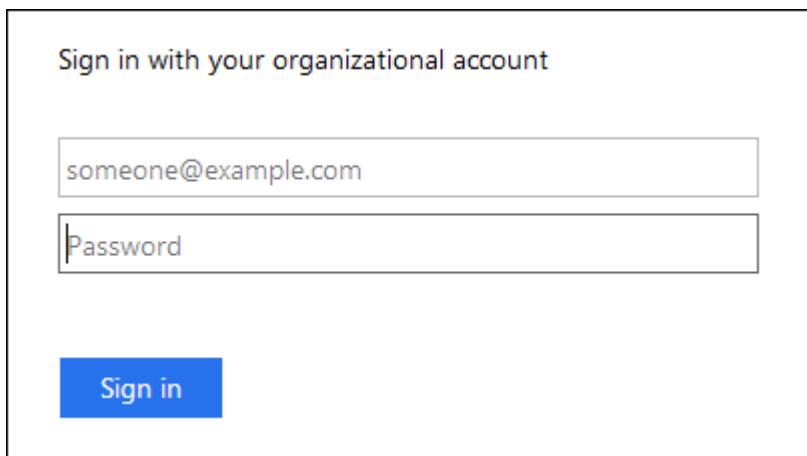
- If SSO is enabled for your StorageGRID system and you have previously accessed the Grid Manager or a tenant account:

i. Do either of the following:

- Enter **0** (the account ID for the Grid Manager), and click **Sign in**.
- Select **Grid Manager** if it appears in the list of recent accounts, and click **Sign in**.

ii. Sign in with your standard SSO credentials on your organization's SSO sign-in page. When you are signed in, the home page of the Grid Manager appears, which includes the Dashboard. To learn what information is provided, see "Viewing the Dashboard" in the instructions for monitoring and troubleshooting StorageGRID.
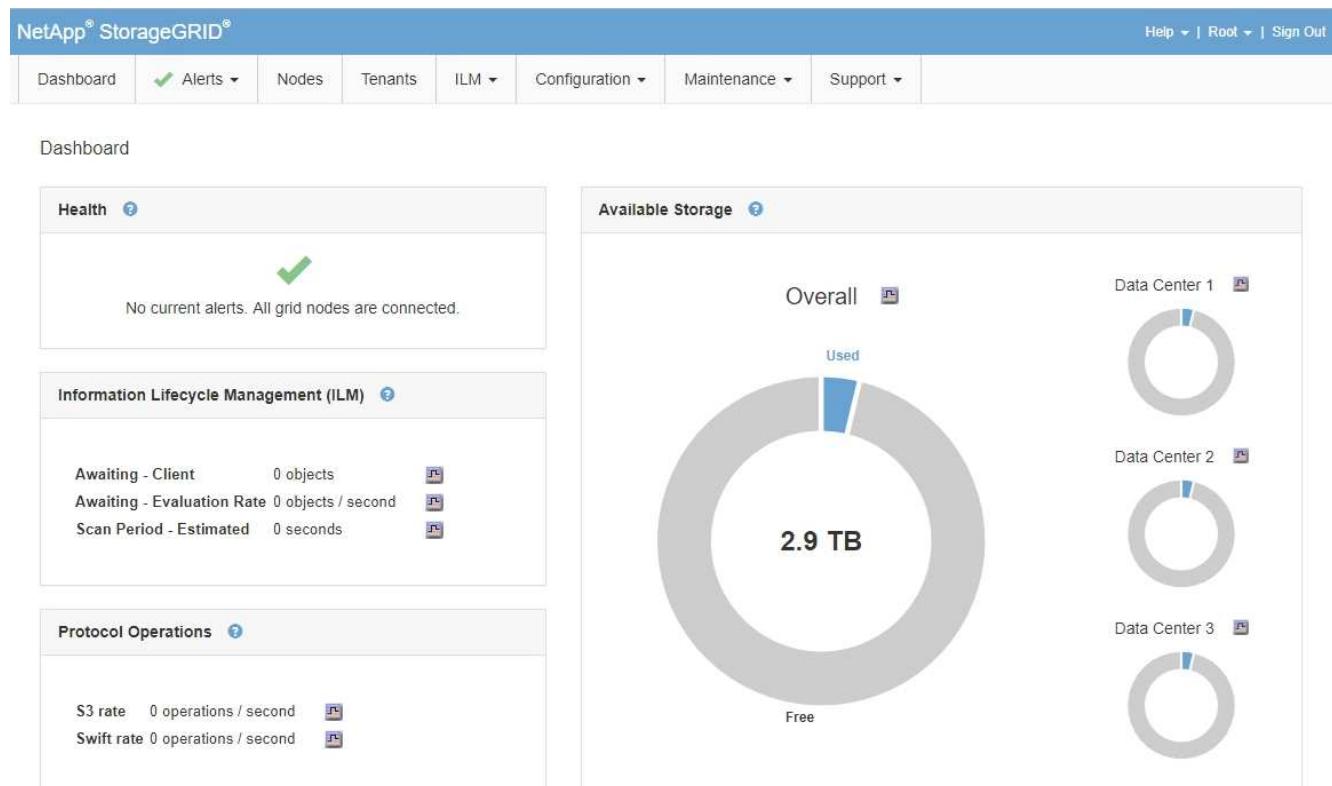
5. If you want to sign in to another Admin Node:

Option	Steps
SSO not enabled	a. In the browser's address bar, enter the fully qualified domain name or IP address of the other Admin Node. Include the port number as required. b. Enter your username and password for the Grid Manager. c. Click **Sign In**.
SSO enabled	In the browser's address bar, enter the fully qualified domain name or IP address of the other Admin Node. If you have signed in to one Admin Node, you can access other Admin Nodes without having to sign in again. However, if your SSO session expires, you are prompted for your credentials again. **Note:** SSO is not available on the restricted Grid Manager port. You must use the default HTTPS port (443) if you want users to authenticate with single sign-on.

Related information

[Web browser requirements](#)

[Controlling access through firewalls](#)

[Configuring server certificates](#)

[Configuring single sign-on](#)

[Managing admin groups](#)

[Managing high availability groups](#)

[Use a tenant account](#)

[Monitor & troubleshoot](#)

Signing out of the Grid Manager

When you are done working with the Grid Manager, you must sign out to ensure that unauthorized users cannot access the StorageGRID system. Closing your browser might not sign you out of the system, based on browser cookie settings.

Steps

1. Locate the **Sign Out** link in the top-right corner of the user interface.
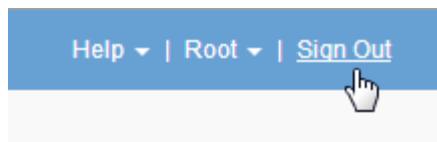
2. Click **Sign Out**.

Option	Description
SSO not in use	You are signed out of the Admin Node. The Grid Manager sign in page is displayed. **Note:** If you signed into more than one Admin Node, you must sign out of each node.
SSO enabled	You are signed out of all Admin Nodes you were accessing. The StorageGRID sign in page is displayed. **Grid Manager** is listed as the default in the **Recent Accounts** drop-down, and the **Account ID** field shows 0. **Note:** If SSO is enabled and you are also signed in to the Tenant Manager, you must also sign out of the tenant account to sign out of SSO.

Related information

Configuring single sign-on

Use a tenant account

Changing your password

If you are a local user of the Grid Manager, you can change your own password.

What you'll need

You must be signed in to the Grid Manager using a supported browser.

About this task

If you sign in to StorageGRID as a federated user or if single sign-on (SSO) is enabled, you cannot change your password in Grid Manager. Instead, you must change your password in the external identity source, for example, Active Directory or OpenLDAP.

Steps

1. From the Grid Manager header, select *your name* > **Change password**.

2. Enter your current password.

3. Type a new password.

   Your password must contain at least 8 and no more than 32 characters. Passwords are case-sensitive.

4. Re-enter the new password.

5. Click **Save**.

Changing the provisioning passphrase

Use this procedure to change the StorageGRID provisioning passphrase. The passphrase is required for recovery, expansion, and maintenance procedures. The passphrase is also required to download Recovery Package backups that include the grid topology information and encryption keys for the StorageGRID system.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.

- You must have Maintenance or Root Access permissions.

- You must have the current provisioning passphrase.

About this task

The provisioning passphrase is required for many installation and maintenance procedures, and for downloading the Recovery Package. The provisioning passphrase is not listed in the `Passwords.txt` file. Make sure to document the provisioning passphrase and keep it in a safe and secure location.

Steps

1. Select **Configuration** > **Access Control** > **Grid Passwords**.
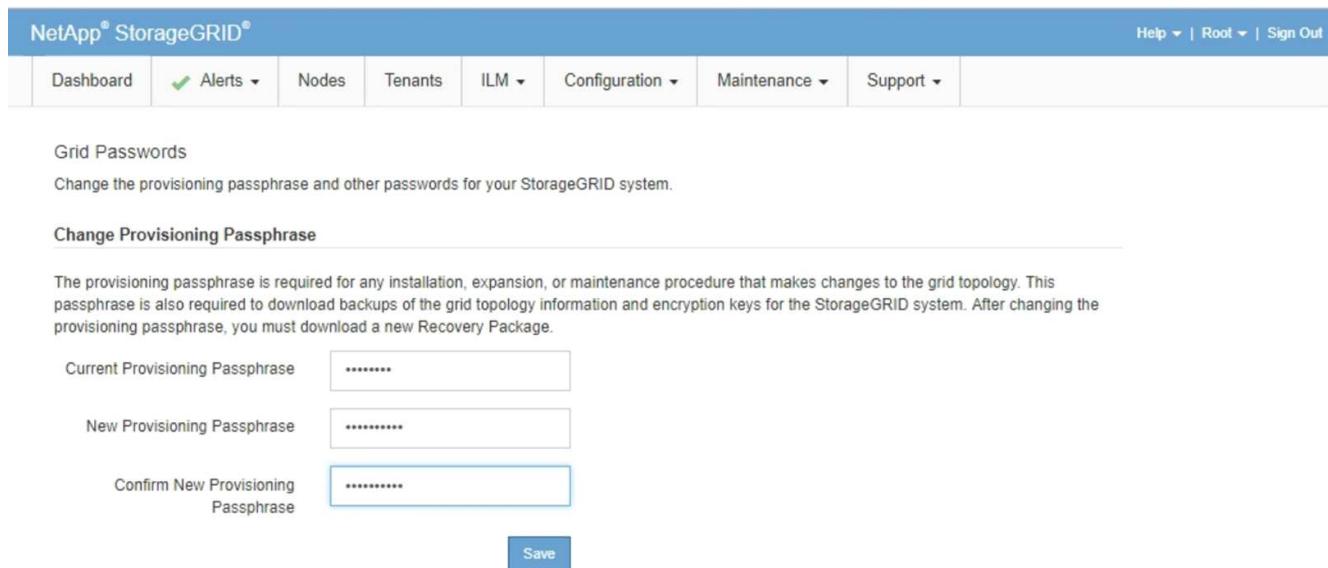

2. Enter your current provisioning passphrase.

3. Enter the new passssphrase.The passphrase must contain at least 8 and no more than 32 characters. Passphrases are case-sensitive.

> ⚠️ Store the new provisioning passphrase in a secure location. It is required for installation, expansion, and maintenance procedures.

4. Re-enter the new passphrase, and click **Save**.

The system displays a green success banner when the provisioning passphrase change is complete. The change should take less than a minute.
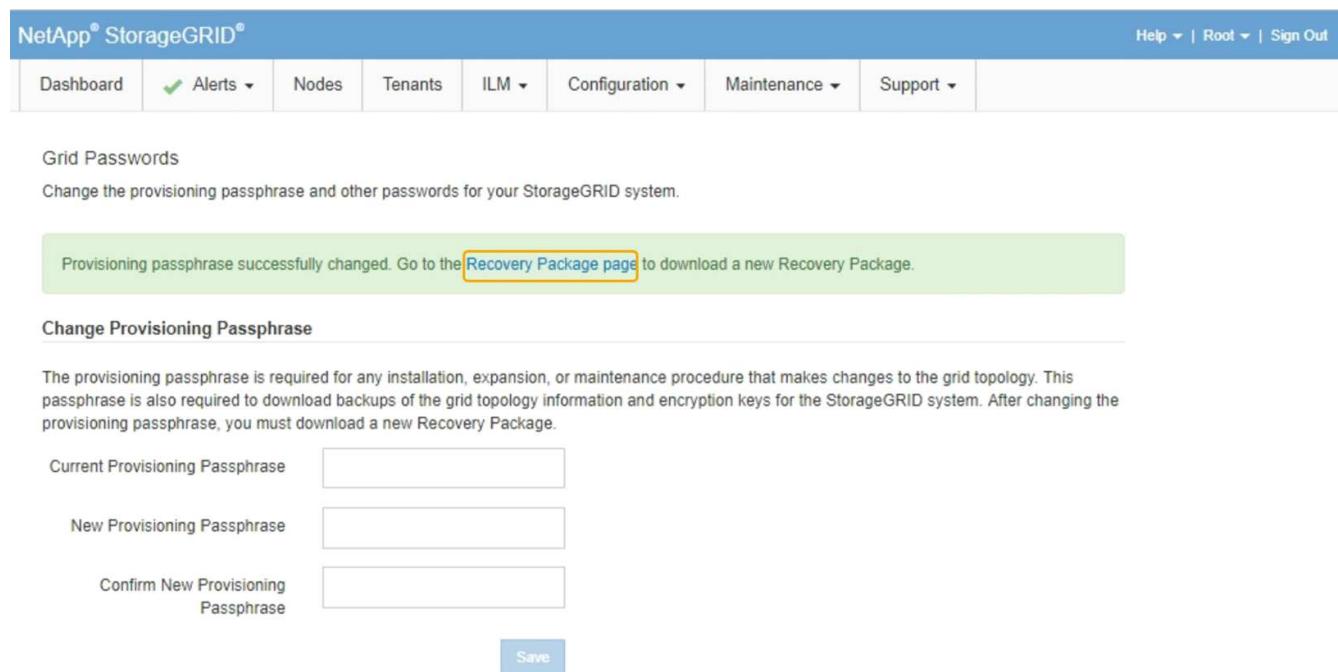
5. Select the **Recovery Package page** link inside the success banner.

6. Download the new Recovery Package from the Grid Manager. Select **Maintenance** > **Recovery Package** and enter the new provisioning passphrase.

> ⚠️ After changing the provisioning passphrase, you must immediately download a new Recovery Package. The Recovery Package file allows you to restore the system if a failure occurs.

Changing the browser session timeout

You can control whether Grid Manager and Tenant Manager users are signed out if they are inactive for more than a certain amount of time.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.

About this task

The GUI Inactivity Timeout defaults to 900 seconds (15 minutes). If a user's browser session is not active for this amount of time, the session times out.

As required, you can increase or decrease the timeout period by setting the GUI Inactivity Timeout display option.

If single sign-on (SSO) is enabled and a user's browser session times out, the system behaves as if the user clicked **Sign Out** manually. The user must reenter their SSO credentials to access StorageGRID again.

> ℹ️ User session timeout can also be controlled by the following:
>
> - A separate, non-configurable StorageGRID timer, which is included for system security. By default, each user's authentication token expires 16 hours after the user signs in. When a user's authentication expires, that user is automatically signed out, even if the value for the GUI Inactivity Timeout has not been reached. To renew the token, the user must sign back in.
> - Timeout settings for the identity provider, assuming SSO is enabled for StorageGRID.

Steps

1. Select **Configuration** > **System Settings** > **Display Options**.
2. For **GUI Inactivity Timeout**, enter a timeout period of 60 seconds or more.

   Set this field to 0 if you do not want to use this functionality. Users are signed out 16 hours after they sign in, when their authentication tokens expire.

   Display Options
   Updated: 2017-03-09 20:36:53 MST
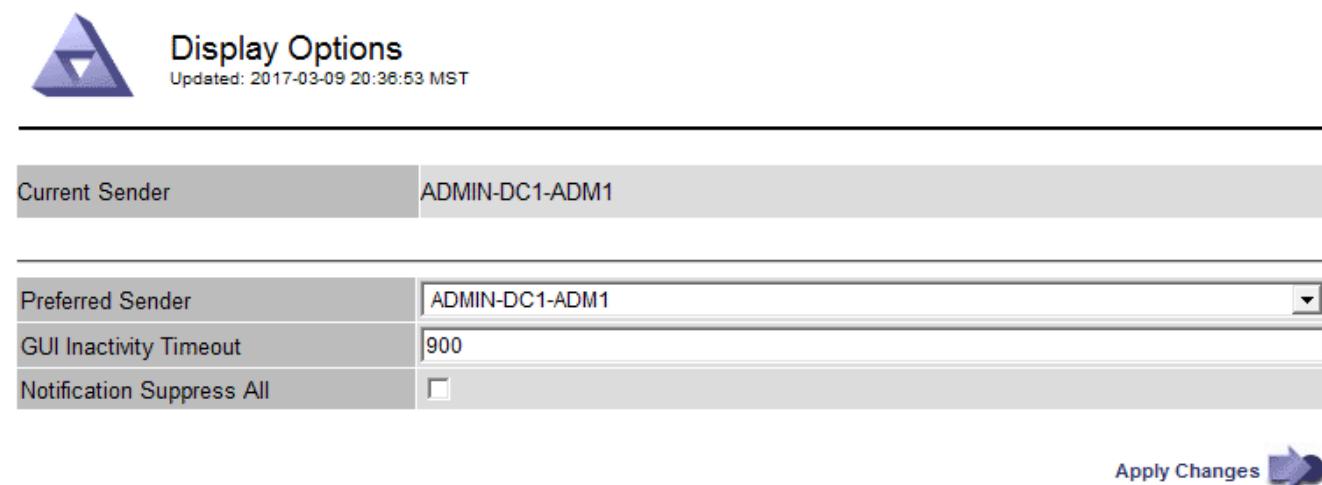
Current Sender	ADMIN-DC1-ADM1

Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	☐

   Apply Changes ➡️

3. Click **Apply Changes**.

   The new setting does not affect currently signed in users. Users must sign in again or refresh their browsers for the new timeout setting to take effect.

Related information

How single sign-on works

Use a tenant account

Viewing StorageGRID license information

You can view the license information for your StorageGRID system, such as the maximum storage capacity of your grid, whenever necessary.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.

About this task

If there is an issue with the software license for this StorageGRID system, the Health panel on the Dashboard includes a License Status icon and a **License** link. The number indicates how many license-related issues there are.

Dashboard

Step

To view the license, do one of the following:

- From the Health panel on the Dashboard, click the License status icon or the **License** link. This link appears only if there is an issue with the license.
- Select **Maintenance** > **System** > **License**.

The License Page appears and provides the following, read-only information about the current license:

- StorageGRID system ID, which is the unique identification number for this StorageGRID installation
- License serial number
- Licensed storage capacity of the grid
- Software license end date
- Support service contract end date
- Contents of the license text file

> ⓘ For licenses issued before StorageGRID 10.3, the licensed storage capacity is not included in the license file, and a "See License Agreement" message is displayed instead of a value.

Updating StorageGRID license information

You must update the license information for your StorageGRID system any time the terms of your license change. For example, you must update the license information if you purchase additional storage capacity for your grid.

What you'll need

- You must have a new license file to apply to your StorageGRID system.
- You must have specific access permissions.
- You must have the provisioning passphrase.

Steps

1. Select **Maintenance** > **System** > **License**.

2. Enter the provisioning passphrase for your StorageGRID system in the **Provisioning Passphrase** text box.

3. Click **Browse**.

4. In the Open dialog box, locate and select the new license file (`.txt`), and click **Open**.

   The new license file is validated and displayed.

5. Click **Save**.

Using the Grid Management API

You can perform system management tasks using the Grid Management REST API instead of the Grid Manager user interface. For example, you might want to use the API to automate operations or to create multiple entities, such as users, more quickly.

The Grid Management API uses the Swagger open source API platform. Swagger provides an intuitive user interface that allows developers and non-developers to perform real-time operations in StorageGRID with the API.

Top-level resources

The Grid Management API provides the following top-level resources:

- `/grid`: Access is restricted to Grid Manager users and is based on the configured group permissions.

- `/org`: Access is restricted to users who belong to a local or federated LDAP group for a tenant account. For details, see the information about using tenant accounts.

- `/private`: Access is restricted to Grid Manager users and is based on the configured group permissions. These APIs are intended for internal use only and are not publicly documented. These APIs are also subject to change without notice.

Related information

Use a tenant account

Prometheus: Query basics

Grid Management API operations

The Grid Management API organizes the available API operations into the following sections.

- **accounts** — Operations to manage storage tenant accounts, including creating new accounts and retrieving storage usage for a given account.

- **alarms** — Operations to list current alarms (legacy system), and return information about the health of the grid, including the current alerts and a summary of node connection states.

- **alert-history** — Operations on resolved alerts.

- **alert-receivers** — Operations on alert notification receivers (email).

- **alert-rules** — Operations on alert rules.
- **alert-silences** — Operations on alert silences.
- **alerts** — Operations on alerts.
- **audit** — Operations to list and update the audit configuration.
- **auth** — Operations to perform user session authentication.

  The Grid Management API supports the Bearer Token Authentication Scheme. To sign in, you provide a username and password in the JSON body of the authentication request (that is, `POST /api/v3/authorize`). If the user is successfully authenticated, a security token is returned. This token must be provided in the header of subsequent API requests ("Authorization: Bearer *token*").

  > (i) If single sign-on is enabled for the StorageGRID system, you must perform different steps to authenticate. See "Authenticating in to the API if single sign-on is enabled."

  See "Protecting against Cross-Site Request Forgery" for information on improving authentication security.

- **client-certificates** — Operations to configure client certificates so that StorageGRID can be accessed securely using external monitoring tools.
- **config** — Operations related to the product release and versions of the Grid Management API. You can list the product release version and the major versions of the Grid Management API supported by that release, and you can disable deprecated versions of the API.
- **deactivated-features** — Operations to view features that might have been deactivated.
- **dns-servers** — Operations to list and change configured external DNS servers.
- **endpoint-domain-names** — Operations to list and change endpoint domain names.
- **erasure-coding** — Operations on Erasure Coding profiles.
- **expansion** — Operations on expansion (procedure-level).
- **expansion-nodes** — Operations on expansion (node-level).
- **expansion-sites** — Operations on expansion (site-level).
- **grid-networks** — Operations to list and change the Grid Network List.
- **grid-passwords** — Operations for grid password management.
- **groups** — Operations to manage local Grid Administrator Groups and to retrieve federated Grid Administrator Groups from an external LDAP server.
- **identity-source** — Operations to configure an external identity source and to manually synchronize federated group and user information.
- **ilm** — Operations on information lifecycle management (ILM).
- **license** — Operations to retrieve and update the StorageGRID license.
- **logs** — Operations for collecting and downloading log files.
- **metrics** — Operations on StorageGRID metrics including instant metric queries at a single point in time and range metric queries over a range of time. The Grid Management API uses the Prometheus systems monitoring tool as the backend data source. For information about constructing Prometheus queries, see the Prometheus web site.

  > (i) Metrics that include *private* in their names are intended for internal use only. These metrics are subject to change between StorageGRID releases without notice.

- **node-health** — Operations on node health status.
- **ntp-servers** — Operations to list or update external Network Time Protocol (NTP) servers.
- **objects** — Operations on objects and object metadata.
- **recovery** — Operations for the recovery procedure.
- **recovery-package** — Operations to download the Recovery Package.
- **regions** — Operations to view and create regions.
- **s3-object-lock** — Operations on global S3 Object Lock settings.
- **server-certificate** — Operations to view and update Grid Manager server certificates.
- **snmp** — Operations on the current SNMP configuration.
- **traffic-classes** — Operations for traffic classification policies.
- **untrusted-client-network** — Operations on the untrusted Client Network configuration.
- **users** — Operations to view and manage Grid Manager users.

Issuing API requests

The Swagger user interface provides complete details and documentation for each API operation.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.

> (i) Any API operations you perform using the API Docs webpage are live operations. Be careful not to create, update, or delete configuration data or other data by mistake.

Steps

1. Select **Help** > **API Documentation** from the Grid Manager header.
2. Select the desired operation.

   When you expand an API operation, you can see the available HTTP actions, such as GET, PUT, UPDATE, and DELETE.

3. Select an HTTP action to see the request details, including the endpoint URL, a list of any required or optional parameters, an example of the request body (when required), and the possible responses.

4. Determine if the request requires additional parameters, such as a group or user ID. Then, obtain these values. You might need to issue a different API request first to get the information you need.

5. Determine if you need to modify the example request body. If so, you can click **Model** to learn the requirements for each field.

6. Click **Try it out**.

7. Provide any required parameters, or modify the request body as required.

8. Click **Execute**.

9. Review the response code to determine if the request was successful.

Grid Management API versioning

The Grid Management API uses versioning to support non-disruptive upgrades.

For example, this Request URL specifies version 3 of the API.

```
https://hostname_or_ip_address/api/v3/authorize
```

The major version of the Tenant Management API is bumped when changes are made that are **not compatible** with older versions. The minor version of the Tenant Management API is bumped when changes are made that **are compatible** with older versions. Compatible changes include the addition of new endpoints or new properties. The following example illustrates how the API version is bumped based on the type of changes made.

Type of change to API	Old version	New version
Compatible with older versions	2.1	2.2
Not compatible with older versions	2.1	3.0

When you install StorageGRID software for the first time, only the most recent version of the Grid Management API is enabled. However, when you upgrade to a new feature release of StorageGRID, you continue to have access to the older API version for at least one StorageGRID feature release.

> ⓘ You can use the Grid Management API to configure the supported versions. See the "config" section of the Swagger API documentation for more information. You should deactivate support for the older version after updating all Grid Management API clients to use the newer version.

Outdated requests are marked as deprecated in the following ways:

- The response header is "Deprecated: true"
- The JSON response body includes "deprecated": true
- A deprecated warning is added to nms.log. For example:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Determining which API versions are supported in the current release

Use the following API request to return a list of the supported API major versions:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Specifying an API version for a request

You can specify the API version using a path parameter (`/api/v3`) or a header (`Api-Version: 3`). If you provide both values, the header value overrides the path value.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protecting against Cross-Site Request Forgery (CSRF)

You can help protect against Cross-Site Request Forgery (CSRF) attacks against StorageGRID by using CSRF tokens to enhance authentication that uses cookies. The Grid Manager and Tenant Manager automatically enable this security feature; other API clients can choose whether to enable it when they sign in.

An attacker that can trigger a request to a different site (such as with an HTTP form POST) can cause certain requests to be made using the signed-in user's cookies.

StorageGRID helps protect against CSRF attacks by using CSRF tokens. When enabled, the contents of a specific cookie must match the contents of either a specific header or a specific POST body parameter.

To enable the feature, set the `csrfToken` parameter to `true` during authentication. The default is `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

When true, a `GridCsrfToken` cookie is set with a random value for sign-ins to the Grid Manager, and the

`AccountCsrfToken` cookie is set with a random value for sign-ins to the Tenant Manager.

If the cookie is present, all requests that can modify the state of the system (POST, PUT, PATCH, DELETE) must include one of the following:

- The `X-Csrf-Token` header, with the value of the header set to the value of the CSRF token cookie.

- For endpoints that accept a form-encoded body: A `csrfToken` form-encoded request body parameter.

See the online API documentation for additional examples and details.

> ⓘ Requests that have a CSRF token cookie set will also enforce the `"Content-Type: application/json"` header for any request that expects a JSON request body as an additional protection against CSRF attacks.

Using the API if single sign-on is enabled

If single sign-on (SSO) has been enabled for your StorageGRID system, you cannot use the standard Authenticate API requests to sign in to and sign out of the Grid Management API or the Tenant Management API.

Signing in to the API if single sign-on is enabled

If single sign-on (SSO) has been enabled, you must issue a series of API requests to obtain an authentication token from AD FS that is valid for the Grid Management API or the Tenant Management API.

What you'll need
- You know the SSO username and password for a federated user who belongs to a StorageGRID user group.
- If you want to access the Tenant Management API, you know the tenant account ID.

About this task
To obtain an authentication token, you can use one of the following examples:

- The `storagegrid-ssoauth.py` Python script, which is located in the StorageGRID installation files directory (`./rpms` for Red Hat Enterprise Linux or CentOS, `./debs` for Ubuntu or Debian, and `./vsphere` for VMware).

- An example workflow of curl requests.

  The curl workflow might time out if you perform it too slowly. You might see the error: A valid SubjectConfirmation was not found on this Response.

  > ⓘ The example curl workflow does not protect the password from being seen by other users.

If you have a URL-encoding issue, you might see the error: Unsupported SAML version.

Steps
1. Select one of the following methods to obtain an authentication token:

   ◦ Use the `storagegrid-ssoauth.py` Python script. Go to step 2.

- Use curl requests. Go to step 3.

2. If you want to use the `storagegrid-ssoauth.py` script, pass the script to the Python interpreter and run the script.

   When prompted, enter values for the following arguments:

   - The SSO username

   - The domain where StorageGRID is installed

   - The address for StorageGRID

   - If you want to access the Tenant Management API, enter tenant account ID.

```
python3 /tmp/storagegrid-ssoauth.py
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
***************************************************************************

***************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

   The StorageGRID authorization token is provided in the output. You can now use the token for other requests, similar to how you would use the API if SSO was not being used.

3. If you want to use curl requests, use the following procedure.

   a. Declare the variables needed to sign in.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

   > (i) To access the Grid Management API, use 0 as `TENANTACCOUNTID`.

   b. To receive a signed authentication URL, issue a POST request to `/api/v3/authorize-saml`, and remove the additional JSON encoding from the response.

   This example shows a POST request for a signed authentication URL for `TENANTACCOUNTID`. The results will be passed to python -m json.tool to remove the JSON encoding.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

The response for this example includes a signed URL that is URL-encoded, but it does not include the additional JSON-encoding layer.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Save the `SAMLRequest` from the response for use in subsequent commands.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Get a full URL that includes the client request ID from AD FS.

One option is to request the login form using the URL from the previous response.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

The response includes the client request ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Save the client request ID from the response.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Send your credentials to the form action from the previous response.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS returns a 302 redirect, with additional information in the headers.

> (i) If multi-factor authentication (MFA) is enabled for your SSO system, the form post will
> also contain the second password or other credentials.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Save the `MSISAuth` cookie from the response.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Send a GET request to the specified location with the cookies from the authentication POST.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

The response headers will contain AD FS session information for later logout usage, and the response
body contains the SAMLResponse in a hidden form field.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzZcYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Save the `SAMLResponse` from the hidden field:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Using the saved `SAMLResponse`, make a StorageGRID `/api/saml-response` request to generate a StorageGRID authentication token.

For `RelayState`, use the tenant account ID or use 0 if you want to sign in to the Grid Management API.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

The response includes the authentication token.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

k. Save the authentication token in the response as `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

You can now use `MYTOKEN` for other requests, similar to how you would use the API if SSO was not being used.

Signing out of the API if single sign-on is enabled

If single sign-on (SSO) has been enabled, you must issue a series of API requests to sign out of the Grid Management API or the Tenant Management API.

About this task

If required, you can sign out of the StorageGRID API simply by logging out from your organization's single logout page. Or, you can trigger single logout (SLO) from StorageGRID, which requires a valid StorageGRID bearer token.

Steps

1. To generate a signed logout request, pass `cookie "sso=true"` to the SLO API:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

A logout URL is returned:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Save the logout URL.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. Send a request to the logout URL to trigger SLO and to redirect back to StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

The 302 response is returned. The redirect location is not applicable to API-only logout.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Delete the StorageGRID bearer token.

Deleting the StorageGRID bearer token works the same way as without SSO. If `cookie "sso=true"` is not provided, the user is logged out of StorageGRID without affecting the SSO state.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` response indicates the user is now signed out.

```
HTTP/1.1 204 No Content
```

Using StorageGRID 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).

An external certificate authority (CA) can issue custom certificates that are fully compliant with your organization's information security policies. StorageGRID also includes a built-in certificate authority (CA) that generates internal CA certificates during system installation. These internal CA certificates are used, by default, to secure internal StorageGRID traffic. Although you can use the internal CA certificates 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.

  System hardening

- 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.

Certificate	Certificate type	Description	Navigation location	Details
Administrator client certificate	Client	Installed on each client, allowing StorageGRID to authenticate external client access. • Allows authorized external clients to access the StorageGRID Prometheus database. • Allows secure monitoring of StorageGRID using external tools.	**Configuration** > **Access Control** > **Client Certificates**	Configuring administrator client certificates
Identity federation certificate	Server	Authenticates the connection between StorageGRID and an external Active Directory, OpenLDAP, or Oracle Directory Server.Used for identity federation, which allows admin groups and users to be managed by an external system.	**Configuration** > **Access Control** > **Identity Federation**	Using identity federation
Single sign-on (SSO) certificate	Server	Authenticates the connection between Active Directory Federation Services (AD FS) and StorageGRID that is used for single sign-on (SSO) requests.	**Configuration** > **Access Control** > **Single Sign-on**	Configuring single sign-on

Certificate	Certificate type	Description	Navigation location	Details
Key management server (KMS) certificate	Server and client	Authenticates the connection between StorageGRID and an external key management server (KMS), which provides encryption keys to StorageGRID appliance nodes.	**Configuration** > **System Settings** > **Key Management Server**	Adding a key management server (KMS)
Email alert notification certificate	Server and client	Authenticates the connection between an SMTP email server and StorageGRID that is used for alert notifications. • If communications with the SMTP server requires Transport Layer Security (TLS), you must specify the email server CA certificate. • Specify a client certificate only if the SMTP email server requires client certificates for authentication.	**Alerts** > **Email Setup**	Monitor & troubleshoot

Certificate	Certificate type	Description	Navigation location	Details
Load balancer endpoint certificate	Server	Authenticates the connection between S3 or Swift clients and the StorageGRID Load Balancer service on Gateway Nodes or Admin Nodes. You 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. **Note:** The load balancer certificate is the most used certificate during normal StorageGRID operation.	**Configuration** > **Network Settings** > **Load Balancer Endpoints**	• Configuring load balancer endpoints • Creating a load balancer endpoint for FabricPool Configure StorageGRID for FabricPool

Certificate	Certificate type	Description	Navigation location	Details
Management Interface Server Certificate	Server	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. This certificate also authenticates Grid Management API and Tenant Management API connections. You can use the internal CA certificate or upload a custom certificate.	**Configuration** > **Network Settings** > **Server Certificates**	• Configuring server certificates • Configuring a custom server certificate for the Grid Manager and the Tenant Manager
Cloud Storage Pool endpoint certificate	Server	Authenticates the connection from the 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.	**ILM** > **Storage Pools**	Manage objects with ILM
Platform services endpoint certificate	Server	Authenticates the connection from the StorageGRID platform service to an S3 storage resource.	**Tenant Manager** > **STORAGE (S3)** > **Platform services endpoints**	Use a tenant account

Certificate	Certificate type	Description	Navigation location	Details
Object Storage API Service Endpoint Server Certificate	Server	Authenticates secure S3 or Swift client connections to the Local Distribution Router (LDR) service on a Storage Node or to the deprecated Connection Load Balancer (CLB) service on a Gateway Node.	**Configuration** > **Network Settings** > **Load Balancer Endpoints**	Configuring a custom server certificate for connections to the Storage Node or the CLB service

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.