

## Provisioner REST API Overview for KumoScale 3.22

The KumoScale™ Provisioner REST API is the primary public interface to KumoScale software. It allows users to manage the pool of KumoScale storage nodes (also known as backends), and to allocate, connect, monitor, and manage storage volumes.

This document specifies the detailed requests/responses/JavaScript Object Notation (JSON) structures of the KumoScale™ Provisioner Representational State Transfer Application Programming Interface (REST API).

All KumoScale Provisioner API commands are supported on implementations in appliance and managed modes.

### NOTES:

- GET responses may have additional fields, which are not described in this document. Those fields are usually for internal usage and should be ignored if not mentioned in the API description.
- Unrecognized JSON fields in POST requests will be ignored by the KumoScale engine.
- All IP addresses provided in this document are for example purposes only.
- Port 30100 is used to access the Provisioner in Appliance mode. See the [Installation Guide for Managed Mode](#) for information on setting the port for Managed Mode.
- Port 443 is used for all authentication functions.

### KumoScale Rest API Security

KumoScale REST API calls are authenticated with basic authentication. There are two different ways to provide authentication: using either a username and password or a token. The username and password may be configured locally, if the authentication mode is set to local, or via Lightweight Directory Access Protocol (LDAP), when authentication mode is set to LDAP or via OpenID Connect (OIDC) when the authentication mode is set to OPEN\_IDC. See the Security chapter of the KumoScale Storage Node REST API for more information.

For security, all calls to the API are made with a .pem file and an access token. The .pem file should be provided with your KumoScale software download.

#### Access with Username and Password

The format is user and password separated by “:” converted to base 64. An example of a valid header:

```
"Authorization: Basic YW#####="
```

An example of calling get users with username **admin** and password **test123!!**:

```
curl -u admin:test123!! -k --cert ./ssdtoolbox.pem https://192.0.2.0/SSDAgentServer/NVMEOF/v1/users
```

#### Access with a Token

An access token is created by accessing the VIP of the storage cluster and using the generate token command. This command generates a token for access to REST operations by copying the token and inserting it into the REST commands until it expires. For example:

```
curl -k --cert ./ssdtoolbox.pem -i -X POST -H 'Content-Type: application/json' -d '{"user":"admin", "expiration":"28800"}' https://192.0.2.0/SSDAgentServer/NVMEOF/v1/executeCommand/GENERATE_TOKEN
```

Where:

- **name** is the RBAC username
- **password** is the password of the RBAC user

Provide a token in the header. The following is an example of a valid header:

```
"Authorization: Bearer eyJ#####"
```

Example of calling get users with a token:

```
curl -H "Authorization: Bearer eyJ##### " -k --cert ./ssdtoolbox.pem https://192.0.2.0/SSDAgentServer/NVMEOF/v1/users
```

- The Role Based Access Control (RBAC) may be disabled, by setting the authentication mode to ‘NONE’. This may be done for testing or environments that do not require authentication.
- REST APIs that are public do not require RBAC authentication or authorization.

- The different permissions of each role can be found in [Provisioner REST Commands Authorization Mapping](#)

Next: [KumoScale Provisioner REST API Command Reference](#)

---

---