

## Role Based Access Control (Appliance Mode)

This section on configuring RBAC Users only applies to KumoScale in Appliance mode. It does not apply to Managed mode.

### Creating and Configuring RBAC Users

You may want to allow other users to access storage nodes. To do that, the KumoScale administrator may configure RBAC users either locally, or via an LDAP server. The minimum number of users in the local configuration is one (1), the **admin** user. At any time, a KumoScale administrator, as the **admin** user, may create additional users who are members of different authentication groups or roles. A role is a collection of privileges limited to a defined functional area of KumoScale software. Users can invoke a storage action only if their role is authorized for that action.

#### RBAC User Roles

Below is a list of the roles and corresponding activities available in KumoScale:

Role Name	Role Description/Privileges
ADMIN	<div>The administrator of the appliance.</div> <div><ul style="list-style-type: none"><li>Can execute all operations.</li><li>Can create and delete users.</li><li>Only a single user can function in this role.</li></ul></div>
STORAGE	<div>Authorized to do storage operations.</div> <div><ul style="list-style-type: none"><li>Should be knowledgeable in orchestration (for example, Kubernetes CSI, Ansible playbooks, or OpenStack).</li></ul></div>
STORAGE_EXPERT	<div>Authorized to do storage operations with access to extended APIs. Extended APIs include support for creating and managing volumes and snapshots.</div> <div><ul style="list-style-type: none"><li>Should be knowledgeable in orchestration (for example, Kubernetes CSI, Ansible playbooks, or OpenStack).</li></ul></div>
NETWORK	<div>Authorized to do network operations.</div> <div><ul style="list-style-type: none"><li>This should be a network administrator.</li></ul></div>
MONITOR	<div>Authorized to only observe information.</div> <div><ul style="list-style-type: none"><li>Should be knowledgeable about telemetry or monitor servers.</li></ul></div>

**Note:** If the admin password is forgotten, administrators must contact a KIOXIA support engineer to reset the password. In this case, contact your local KIOXIA support representative for assistance.

#### User Account Requirements

The administrator (**admin**) may configure up to thirty-two (32) users under Local authentication. Once the user is created, the password may be changed using the REST API **Modify Password** command. Only the user is allowed to change their own password; the administrator cannot change the password for anyone but admin.

##### Username Requirements

- Up to sixteen (16) alphanumeric characters.
- Must be unique.

Local usernames are not case-sensitive.

##### Password Requirements

Password requirements are defined according to the OS password policy. Password characters do not appear on the screen

#### LDAP Server Authentication

LDAP authentication requires configuring an LDAP server.

- KumoScale software supports integration to a single LDAP server. Use add, modify, or remove **LDAP** commands to configure server access.
- The **certificate-upload** command should be used by administrators to upload LDAP certificate files to establish a secure connection (working with **LDAP TLS** or **LDAPS**).
- The set authentication mode command is used to set the authentication mode to **LDAP**.

Usernames and passwords are configured via the LDAP server for REST APIs only.

Authentication with Tokens

In addition to the local user account, users need to generate **JavaScript™ Object Notation (JSON) Web Tokens (JWT)** to access the KumoScale Provisioner and other interfaces. These tokens are issued using the KumoScale REST API *Generate Token* command and may be issued by any user. The token gives you access to the storage node and Provisioner for a limited period. This is described further in [Authentication](#).

Next: [Authentication](#)

---

---