Access Management

Dremio allows for the implementation of granular-level privileges, which defines a user/role's access privilege and available actions for specific objects, such as a dataset, project, or cloud. This is called access management, and gives administrators the ability to restrict access to any object in Dremio.

The following features are available:

- **Privileges:** Privileges enable users to perform explicit operations on objects in Dremio. Additionally, privileges may be set on individual datasets (tables or views) or whole schemas, allowing for a simplified configuration with larger catalogs. To learn more about the Dremio object model, see Objects in Dremio Cloud.
- **Row-access and column-masking policies:** Row-access and column-masking policies enable you to grant users access to particular rows or columns.
- **Flexible Management:** Privileges can be easily configured using GRANT TO USER command, GRANT TO ROLE command, GRANT ROLE command, REST APIs, and an intuitive and easy-to-use user interface.
- **Ownership:** An object-oriented model allows for a clearly-defined and transferable owner for all aspects in Dremio, including cloud and engine configuration. Users with ownership over an object will automatically retain all privileges necessary to modify the object and read/write its data.
- **Users** & **Roles:** Administrators may create and manage identities in Dremio or using external identity providers (IdP).

The following topics cover the various aspects of access management, along with instructions for how to apply privileges via Dremio:

- Best Practices
- Privileges
- Roles
- Row & Column Policies
- SCIM
- Users

The following SQL commands may be used from the SQL Runner:

- GRANT TO USER
- GRANT TO ROLE

- CREATE USER
- REVOKE FROM ROLE
- REVOKE FROM USER
- REVOKE ROLE

Was this page helpful? Yes No