Create A Security Dimension

You can restrict users to access only a subset of data in a cube by creating one or more security dimensions. When users run queries against the cube, AtScale uses the security dimension as a runtime constraint. However, the constraint does not appear as part of the query on the AtScale Queries search page.

Introduction

A security dimension consists of the following:

- **Security Dimension Dataset:** A table or dataset that relates user IDs to rows in either dimension or fact datasets. See Mapping table example.
- **Attribute Filter Key Column:** The column of the security dataset used to filter either a dimension or fact dataset.
- **Column Containing IDs:** The column of the security dataset that contains AtScale user/group login ids.
- **Scope:** Determines what queries the security dimension is applied to. The three values: Related, Fact, and All are described below.
- **Lookup Rules:** Provides control over the security enforcement query pattern. Some data warehouses perform better with the "Use Filter Key" option.

  1. **None:** The system will enforce security by joining with the security dimension table.
  2. **Use Filter Key:** The system will enforce security by first looking up the Filter Key Column values using the User's id and then use those values as a constraint in a second query against the fact or dimension dataset.

When a user runs a query that conforms to the specified scope setting, the AtScale engine will enforce the security by either adding joins or by performing preliminary lookup queries, depending on the configured Lookup Rule.

Restrictions

Consider the following:

- Data access by super users is not restricted by security dimension tables. These users have full access to the data in cubes that are in projects that they are granted access to.
- Usernames for users that access security dimensions must be in lowercase, unless you configure AtScale to normalize their usernames to lowercase automatically. To enable the automatic normalization of user names, follow these steps:

1. Log in to Design Center as an AtScale super user or Organization Administrator
2. From the Design Center menu bar (top of page), select **SETTINGS > ENGINE**.
3. Scroll down to the `auth.user.normalize.lowercase` setting and set to **True**.
4. Restart the engine.

More Information

- ▲ Setting the scope
- ▲ Mapping table example
- ▲ Creating a User-Based Security Dimension
- ▲ Creating a Group-Based Security Dimension
- ▲ Editing and Removing Security Dimensions