Row Security Objects

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

Introduction

A row security object consists of the following:

- **Security Dataset:** A table or dataset that relates user/group IDs to rows in either dimension or fact datasets. See Mapping table example.
- **Attribute Filter Keys:** The column(s) of the security dataset used to filter either a dimension or fact dataset.
- **IDs:** The column of the security dataset that contains AtScale user/group IDs.
- **Scope:** Determines what queries the security dimension is applied to: Related, Fact, or All. These values are described in Setting the Scope.
- **Lookup Rules:** Provides control over the security enforcement query pattern:
    - **None:** The system enforces security by joining with the row security table.
    - **Use Filter Key:** The system enforces security by first looking up the **Filter Key Column** values using the user/group IDs, then use those values as a constraint in a second query against the fact or dimension dataset. Some data warehouses perform better with this option.

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

Restrictions

Consider the following:

- Data access by super users is not restricted by row security tables. These users have full access to data in models 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:
    1. Log in to Design Center as an AtScale admin.
    2. In the main menu, select **Settings**, then click **Engine** in the **Settings** panel.
    3. Enable the `auth.user.normalize.lowercase` setting.
    4. Click **Save Engine Settings**.
    5. Restart the engine.

More Information

- Setting the scope
- Mapping table example
- Creating a Row Security Object
- Editing and Removing Row Security Objects