Row Security

Row security files enable you to define security objects, which restrict access to data in a model. These restrictions can be configured at either the user or the group level. When users run queries against a model, AtScale uses the `row_security` object as a runtime constraint.

Row security requires a separate dataset that maps user or group IDs to specific rows in a dimension or fact dataset. Each user or group can only access the data in rows that match the filter; for example, you can restrict a user's access to rows relating to specific countries only.

Once you create a security row object, you can use it to secure other dimensions and datasets in a model by creating a relationship from the dataset/dimension you want secured to the security row file. For more information, see Models.

For more information on how security dimensions function in AtScale, see Modeling Row Security Objects.

Row security files support the following properties.

Unique_name

- **Type:** string
- **Required:** Y

The unique name of the security object. This must be unique across the repositories and all subrepositories.

Object_type

- **Type:** const
- **Required:** Y

The type of object defined by the file. For row security files, the value of this property must be `row_security`.

Label

- **Type:** string
- **Required:** Y

The name of the security object, as it appears in AtScale. This value does not need to be unique.

Dataset

- **Type:** string

- **Required:** Y

The dataset that contains the user-to-attribute mappings determining which rows each user/group can access.

Filter_key_column

- **Type:** string
- **Required:** Y

The column in the security dataset that defines the rows each user/group has access to.

Ids_column

- **Type:** string
- **Required:** Y

The column of the security dataset that contains AtScale user/group IDs.

Id_type

- **Type:** string
- **Required:** Y

Determines whether the IDs are for users or groups.

Supported values:

- `user`
- `group`

Scope

- **Type:** string
- **Required:** Y

Determines which queries the security constraint is applied to.

Supported values:

- `related`: The security constraint is applied when the query selects any dimension or secondary attribute that has a path to the security dataset, as long as no fact table is used. The security constraint is not applied to dimension-only queries that select multiple dimensions related through a fact table.

- `fact`: The security constraint is applied to the same queries as the `related` option, as well as queries that include a measure from a fact table connected to the secure dimension. The security constraint is not applied to single-dimension-only queries that are related to the secured dimension via the fact table. However, multi-dimension-only queries do have security applied because they are joined using a synthetic measure from the fact table that relates them.
- `all`: The security constraint is applied to all queries, unless there is no path to the security dimension. This is the case with two separate fact tables, each with their own unrelated dimensions.

Description

- **Type:** string
- **Required:** N

A description of the security object.

Use_filter_key

- **Type:** boolean
- **Required:** N

Determines how AtScale enforces security.

Supported values:

- `true`: The system first looks up the `filter_key_column` values using the user or goup's ID, and then uses those values as a constraint in a second query against the fact dataset or dimension. Some data warehouses perform better with this option.
- `false`: The system enforces security by joining with the security table.

Secure_totals

- **Type:** boolean
- **Required:** N

Enables/disables the secure totals functionality.

When enabled, the security restriction applies to the following:

- Subtotal measures of the secured hierarchy level or reachable attributes of higher levels.
- Queries that select secured fact tables (a `scope` of `all` or `fact`), but do not select the secured dimension.

- The grouping of the secured level.
- The secured level's secondary attributes.
- Attributes and nested dimensions that are reachable from hierarchy levels lower than the secured level.

When secured totals is disabled, the security restriction only applies to the following:

- The grouping of the secured level.
- The secured level's secondary attributes.
- Attributes and nested dimensions that are reachable from hierarchy levels lower than the secured level.

Supported values:

- `true` (default)
- `false`