GroveStreams Access Permissions Guide

Table of Contents

Overview

GroveStreams Access Permission settings on GroveStreams repository objects are used to grant or deny access or actions for specific Groups. This allows for:

- Securing sensitive data from unwarranted access while allowing necessary data to be available to all relevant users
- Controlling capabilities.

GroveStreams Access Permissions

- **Read**:
  - View all Properties of an object
- **Write**:
  - Modify an object
  - Create objects in a folder
  - Move objects to or from a folder
    - Write permission is required for the source and destination folders
  - Add, delete, modify stream samples
- **Delete**
  - Delete an Object or folder contents
  - Prevents delete of a folder if any children do not have delete permission
  - Does not prevent add, delete, modify of stream samples. Use Write permission instead.
- **Execute**
  - Run objects such as Stream Aggregation and Runnables
- **Modify Permissions**
  - Read and modify the security settings for an object
- **Traverse**
  - View the contents of a folder

GroveStreams Group Membership

A user assumes the combined access permissions of all the groups defined for an object of which the user is a member (explicit or implicit)

Granted and Denied Access

Denied Access has precedence over Granted Access

Travers Access

A user must have Traverse access permission on all of the ancestors of the object to access the object.

Ownership of Object

The owner of an object has full access permissions to the object (but still requires traverse access).

Access Permission Inheritance

Access permissions on a content repository object are, by default, inherited by its parent. To assign different permissions on an object, check the 'Include inheritable permissions from parent' option on the security tab.

The inheritance of security settings makes administration easier when dealing with a large number of objects. With a well thought out organization of the repository objects, only a single ancestor's security will need to change. Adding or moving objects, with inheritance enabled, will allow the objects to assume the security settings of the new parent folder.

However, when security is overridden at lower levels in the hierarchy, it becomes difficult to determine where these overrides exist and what impact they have.

Managing GroveStreams Capabilities

Access to various functional areas and administrative tasks is controlled through the Capabilities which are assigned to Groups. Users Capabilities are derived from combining all Capabilities from all Groups the user is a member of (implicitly and explicitly).

Capabilities

- Observation Studio
    - Allows access to Observation Studio. This setting removes a link to Observation Studio from the user's start page. Objects within Observation Studio are still accessible such as components, dashboards, and maps.
- System Notifications
    - Allows System Notifications to be viewed and deleted
- Job Notifications
    - Allows Jobs to be viewed
- Delete Jobs
    - Allows Jobs to be deleted or 'deleted and canceled' if the job is still running.
- Manage Organization Settings

    - Allows Organization settings to be edited including:
        - General Settings
        - Public/Private Settings
        - Creating Blueprints
- Manage Users and Groups
    - Allows access to the Users and Groups management window
- Manage X509 Certificates
    - Allow access to X509 certificates window. X509 certificates are required for the MQTT API
- Manage API Keys
    - Allows access to the API Keys management window
- Manage Process Queue
    - Allows access to the process queue management window
- Manage Stream Groups
    - Allows Stream Groups to be viewed, created, edited, and deleted
- Manage Imports
    - Allows access to the Import Profile management window
- View Organization Billing Metrics
    - Allows users to view Billing Metrics for an Organization within the Accounts Usage page
- Execute Action from API
    - Actions are items like sending SMS and emails via the HTTP API using a user session.

Managing Repository Access

The design of security access to GroveStreams content first requires an analysis of the types of data available. Generally, data will be organized at a high level by business unit or functionality, such as by building, campus, region, country. Data may then be classified by employee position. For example, a region manager would have access to all components, dashboards, and maps for campuses and buildings within their region, but a campus manager would only have access to their own campus buildings.

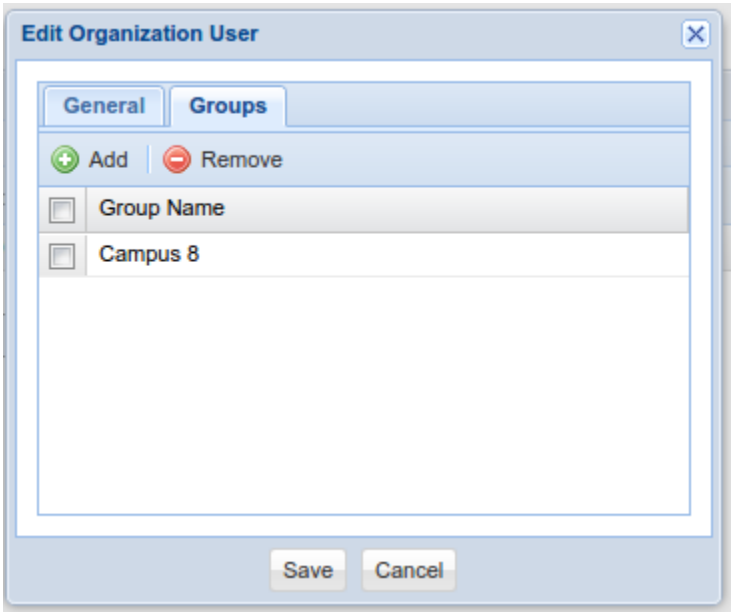
Security should first be assigned within the component repository and then assigned within the content (dashboards and maps) repository.

Groups

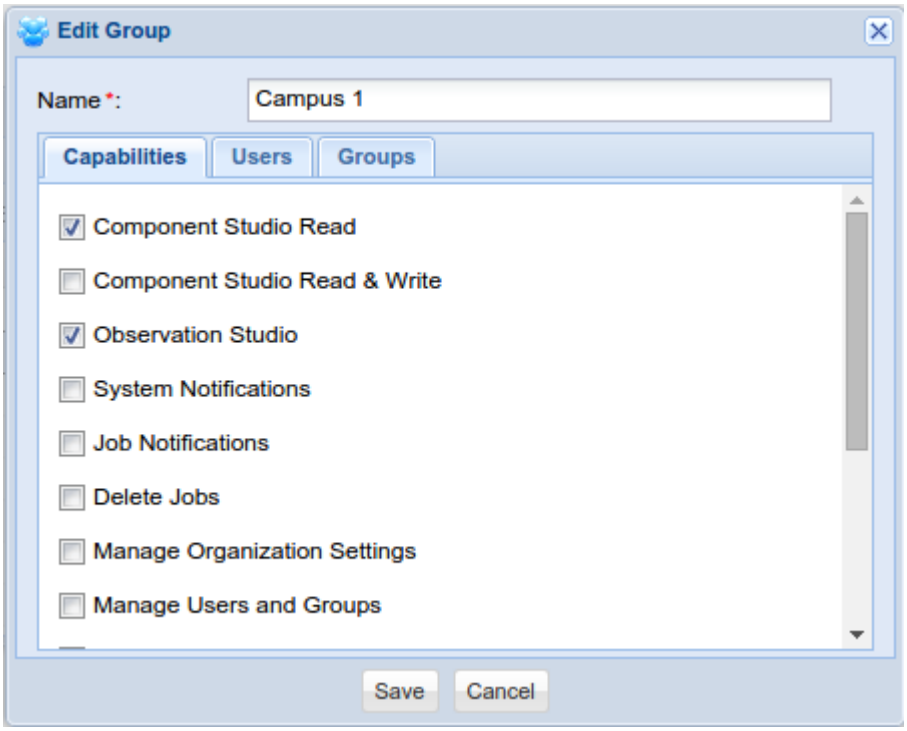
Groups can contain Users or other Groups. When other groups are included:

- All capabilities from other groups and groups they contain (and so on) are aggregated together during capability detection
- Access rights for all groups and groups they contain (and so on) that a user belongs to directly or indirectly are aggregated together during repository access detection
- A user is added to a group in the user editor or in the group editor window.

User Editor Window:



Group Editor Window:



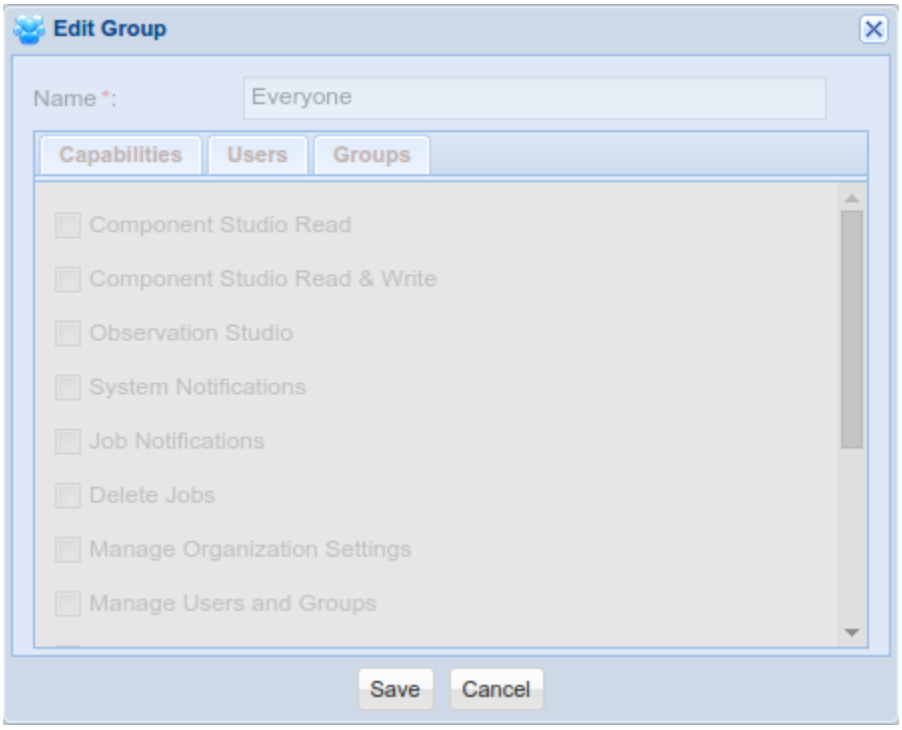
Dashboards, Maps, and Stream Groups

All Components, Streams, and events will be filtered by Component Access Rights while viewing dashboards, maps, and stream group results.

A dashboard with all streams within an organization may be designed with access to everyone. A user will only see the components and streams they have access to when they view the dashboard.

The Everyone Group

The Everyone group is automatically created during the creation of an organization. This group exists to simplify repository access rights administration. It is implied that everyone belongs to the Everyone group when it is included by a content repository for security permissions. The Everyone group is not used for Capabilities detection. The Everyone group cannot be edited or deleted.



The Administration Group

The Administration group is automatically created during the creation of an organization. It cannot be deleted. It is used to assign all capabilities to new users who are considered administrators. These capabilities can be restricted, but it is not recommended.

The Users Group

The Users group is automatically created during the creation of an organization. It has no special features. It can be edited or deleted.

The Organization Owner

The owner of the organization has access to all resources and has all capabilities. Any configured restrictions will be ignored. An organization owner has a few more rights than an Administrator with full capabilities:

- The ability to delete the organization
- The ability to view organization account usage metrics
- Change the ownership of the organization
- Change the Payer of the organization
- Editing of organization within a Branding Group

Blueprints

All access security information is included within a blueprint. The only exception is that Users are not included in a blueprint. Avoid using Users directly when setting up repository rights and use Groups instead. This will ensure your repositories will be created with the correct rights, by groups, when an organization is created from a blueprint.

The **Hierarchy Access Example** below demonstrates using Groups instead of Users directly while configuring rights on each repository folder.

Hierarchy Access Example

We have created a system blueprint with an example of hierarchical access right permissions. To see the example, create a new organization with the system blueprint:

1. Navigate your GroveStream's start page
2. Click the **Create a new organization** button
3. Enter an organization name
4. Expand the **Advanced** section
5. Select **Create with a system blueprint**
6. Choose the **Access Rights Example** blueprint
7. Click **Create Organization**

The **Access Rights Example** organization demonstrates a four level security hierarchy of Components, Country, Region and Campus.

A user only needs to be added to one of the correct groups to assume the proper access rights:

- The organization owner has access to all folders, components, dashboards and maps.
- Users that belong to the Canada group have read-only access for the root folder and total access to Canada and all of its children.
- Users that belong to the Ontario Group have read-only access to folders above Ontario and total access below Ontario.
- Users that belong to the Campus 1 group have read-only access to folders above Campus 1 and total access below Campus 1.

Components and Dashboards are set to inherit rights from their parent. Their rights will automatically change as they are moved to different folders. Newly created Components and Dashboards will inherit

the rights from the parent folder they are created under. Users do not have to setup rights for every new artifact created under a folder since inherit rights is enabled by default for all newly created atrifacts.

Add a new user and try adding the user to a different group to see the results. The same hierarchical rights can be created for the Dashboard and Maps Content Repository.