Access Management Features Overview

Wiki Home	**Grouper Release Announcements**	**Grouper Guides**	**Grouper Deployment Guide**	**Community Contributions**	**Internal Developer Resources**

Access Management Features Overview

See the Grouper Deployment Guide for information on Access Control models.

Grouper provides features to manage access to resources and services. Below are general guidelines on when to use each approach.

How do I set up the privileges determining what a subject can do with a group, such as Admin, Update, Read and View?

These privileges are specified when you define folders, groups and members. See the Grouper training video on How to Design Groups. See also the Grouper Glossary. Use the Grouper Template Wizard to help set up folders, groups and privileges in a consistent manner.

What happens when someone leaves the organization or changes affiliations?

Setup Deprovisioning configuration and deprovision the user who leaves

How can I get reminded to review memberships?

Setup Attestation on a folder or group and get reminders to review the membership of a group

When do I use rules?

Rules are triggers that occur when events happen in Grouper. For example, you would use rules if you want someone to have an end date applied to a membership when another membership is removed (e.g. when a student is out of the classlist, then add a disabled date on the class wiki group for that student). A set of rules use cases is provided.

When do I use hooks?

Hooks are Java code which are executed before or after certain actions in Grouper. There are some optional built in hooks, but custom hooks are generally an advanced topic and if there is a better way to accomplish the goal that would probably be preferable. Discuss the use case with the InCommon-Grouper slack channel to determine the best approach.

How can I get reminded to review memberships?

Setup Attestation on a folder or group and get reminders to review the membership of a group

When do I use attributes and scripts for provisioning?

The **ABAC with scripted groups** feature can offer efficiency in implementing access policies. It's important for the common groups and policy language to be well documented and people to be properly trained. See the information on Attribute Based Access Control (ABAC) with scripted groups.

When do I use roles?

Roles are RBAC objects that are actually just a special type of group.

Keep in mind:

- You need to use a role whenever you assign permissions.
- You can assign permissions to the role, which means that all users who have that role will effectively have that permission.
- Or you can assign permissions directly to the user in the context of the role. This is so shared permissions relate to an application.
  - For example
  - Mary cannot READ the artsAndSciences org.
  - Mary can READ the artsAndSciences org as a user in the payroll system (payrollUser role).
- Note that a role is implemented as a special type of group, though you can think of it as a bridge between users and permissions.
- See additional information in the Grouper training video on Grouper Integration (around minute 3).

When do I use permission limits?

Permission limits are run time constraints on permissions. The permission that has a limit can be assigned to a role or to a subject in the context of a role. The limit can only be assigned to a direct permission assignment, not an inherited one. Generally you will use a limit when there is some information about the context of the user at the time that the permissions query is happening that limits the outcome. For example, if the user can only access the payroll system during business hours, then the time of day is the context. If the user can approve below $2000, then the amount of approval is the context. There are built in limits, or you can implement custom ones. These are implemented as a special type of attribute on the permission assignment, and some Java logic.

When do I use allow/disallow?

Allow/disallow is used when there is inheritance in the permissions due to any of: resource inheritance, action inheritance, role inheritance, membership inheritance, and there is a wider allow, and a narrower disallow. For instance, if the org chart is modeled as permission resources, and there is an allow of "all" for a user in the payroll system, then that user is allowed to see everyone in the payroll system. Maybe that user shouldn't be able to see his/her peers, or executives. You could assign a disallow for the executive org, and for the user's own org. These three assignments will solve the requirement.

When do I use enabled / disabled dates?

Enabled / Disabled Dates are used when the membership or group should be enabled in the future, or disabled after a certain period of time.

S**ee Also**

Role and permission management
Permission Limits
Enabled and disabled dates
Rules
Recent Memberships (Grace Period)

Grouper Template Wizard

Grouper Custom UI Examples

Grouper Custom Templates via GSH

Grouper Subjects in One Group Only

Attribute based access control (ABAC) with scripted groups