Example Access Policies

Example Access Policy 1 - Computing Lab | Example Access Policy 2 - Access to Online Course Material

This section explores several example access policies and how they might be implemented using the strategies described in this guide. They are provided to help reinforce how the concepts in this guide can be used to translate natural language policy into Grouper digital policy. The TIER provisioning state change progression models also provide useful examples.

As a general strategy, each of these examples uses a single access policy group which is itself a composite group of an allow group and deny group. The allow and deny groups may only include reference groups as direct members. These may be centrally managed under the "ref:" folder, maintained by an organization under the "org:" folder, or be application specific reference groups under the "app:" folder. Grouper has many features to automatically manage membership in these groups.

While there are many possible naming strategies that can be used for groups, it is important to be as consistent as possible particularly with ref groups. While not required, these examples also endeavor to minimize embedded punctuation and use camelCase to simplify the reading of long names, using an underscore (i.e. "_") is another common approach.

The examples below are illustrations of "policy groups and static application permissions," as defined in the Access Control Models section.

Example Access Policy 1 - Computing Lab

Policy 1.0 - All students can log on to the computers in the lab.

An access policy group, app:computerLab:labLoginAuthorized is created in Grouper that maps to the lab computer access control mechanism. The ref:student:allStudents group is then added to app:computerLab:labLoginAllow. There is nothing in app:computerLab:labLoginDeny for this example. app:computerLab:labLoginAuthorized is composite group of labLoginAllow minus labLoginDeny.

Access Policy Group	Allow Groups
app:computerLab:labLoginAuthorized	ref:student:allStudents

Policy 1.1 - All students, all teaching faculty and all computer lab administrators can logon to computers in the lab.

In this example, app:computerLab:labLoginAuthorized has some additional members in the app:computerLab:labLoginAllow group. An institutional reference group for teaching faculty, ref:faculty:teachingFaculty is maintained automatically by institutional data. Additionally, an application scoped reference group for lab administrators, app:computing:computingLabManagers, is maintained manually by the computing lab director. Thus three groups are combined by Grouper into the labLoginAuthorized policy group.

Access Policy Group	Allow Groups
	ref:students:allStudents
app:computerLab:labLoginAuthorized	app:computing:computerLabManagers
	ref:faculty:teachingFaculty

Policy 1.2 - Any member of the university community that has been shown to be violating University Computing Policy shall be blocked from access to University Computing Labs. The first offense shall block usage for two weeks. The second offense shall block usage for the remainder of the current semester. The third offense will permanently block the offender's access until an appeal is approved by the Office of the Chief Information Security Officer.

Implementation of this policy requires the addition of a deny group app:computerLab:labLogin_deny. Any subject with membership in the labLogin_deny group will be denied access regardless of membership in other groups. This policy requires three deny groups to represent the three cases:

- app:computerLab:ref:aupViolationFirst
- app:computerLab:ref:aupViolationSecond
- app:computerLab:ref:aup:ViolationThird

Each deny group is added to labLogin_deny. Membership in any one of the three deny groups would effectively deny access. Membership added to aupViolationFirst would be set to expire within two week either manually or by a Grouper Rule. aupViolationSecond has a Grouper rule that clears all membership at the end of the current semester. aupViolationThird is manually managed by the CISO.

Access Policy Group	Allow Groups	Deny Groups
	computingLabManagers	aupViolationSecond
labLogin_authorized	ref:student:all_students	aupViolationFirst
	ref:faculty:teachingFaculty	aupViolationThird

Example Access Policy 2 - Access to Online Course Material

Policy 2.0 - All students of Introductory Physics will use an online text book and excerpts of classical books such as Newton's Principia via the Physics Department's websites. All students except for physics majors will use the current version of the online book (*physics_101_current*), but physics majors will use the newest version (*physics_101_new*) which is not yet thoroughly reviewed.

This policy calls out **two reference groups:**

- physics majors - ref:student:majors:physics:students
- students enrolled in Introductory Physics - ref:course:*term*:physics:101:students

These two reference groups would be automatically kept in sync with institutional data via the Grouper loader.

The policy also calls out three resources that have different access rules, and these are represented by three **access policy groups**.

- The first one, access to Classical Books would be represented by access policy group, app:physics_books:classicalBooks. The allow group, a pp:physics_books:classicalBooksAllow would have both majors:physics:students and physics:101:students as direct members.
- The second policy states the access to the current version of the online textbook is limited to non physics majors enrolled in the course and is represented by access policy group app:physics_books:physics_101_current. The allow group physics_101_current_allow, would contain the class roster, physics:101:students as a direct member, and the deny group, physics_101_current_deny, would contain physics majors, majors :physics:students.
- The third policy states physics majors taking the course should have access to the newest version of the book, and is represented by access policy group, app:physics_books:physics_101_new. The policy can be implemented with a local app specific reference group that takes the intersection of the class roster and physics majors to create app:physics_books:ref:101_physics_majors. The allow group, physics_101_new_ allow, would have app:physics_books:ref:101_physics_majors as a direct member.

Access Policy Group	Allow Groups	Deny Groups
classicalBooks	majors:physics:students physics:101:students	
physics_101_current	physics:101:students	majors:physics:students
physics_101_new	101_physics_majors	

Previous: Conclusion