

Grouper rules privileges inheritance on UI

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

In Grouper 2.3+ there is support for privileges inheritance in the new UI. Inherited privileges were previously available by assigning attributes in a specific way or by using GSH. Note: inherited privileges are also displayed in the normal privilege screens. If they are removed from the object privilege screen, they will be automatically reassigned within a period of time (e.g. within a day, when the rule daemon runs which is configurable).



Grouper Privileges (ADMIN, UPDATE, READ, VIEW, etc.) are defined in the [Grouper Glossary](#).

There are 7 screens to control and view inherited privileges.

- [Patch improvements](#)
- [Screen: View or assign inherited privileges in a folder](#)
- [Screen: View inherited privileges that affect a group](#)
- [Screen: View inherited privileges that affect a folder](#)
- [Screen: View inherited privileges that affect an attribute definition](#)
- [Screen: View inherited privileges that affect a subject](#)
- [Screen: View inherited privileges assigned to members of a group](#)
- [Screen: View all inherited privileges in registry](#)
- [Privileges required to manage inherited privileges](#)

Patch improvements

In grouper newer than these patches:

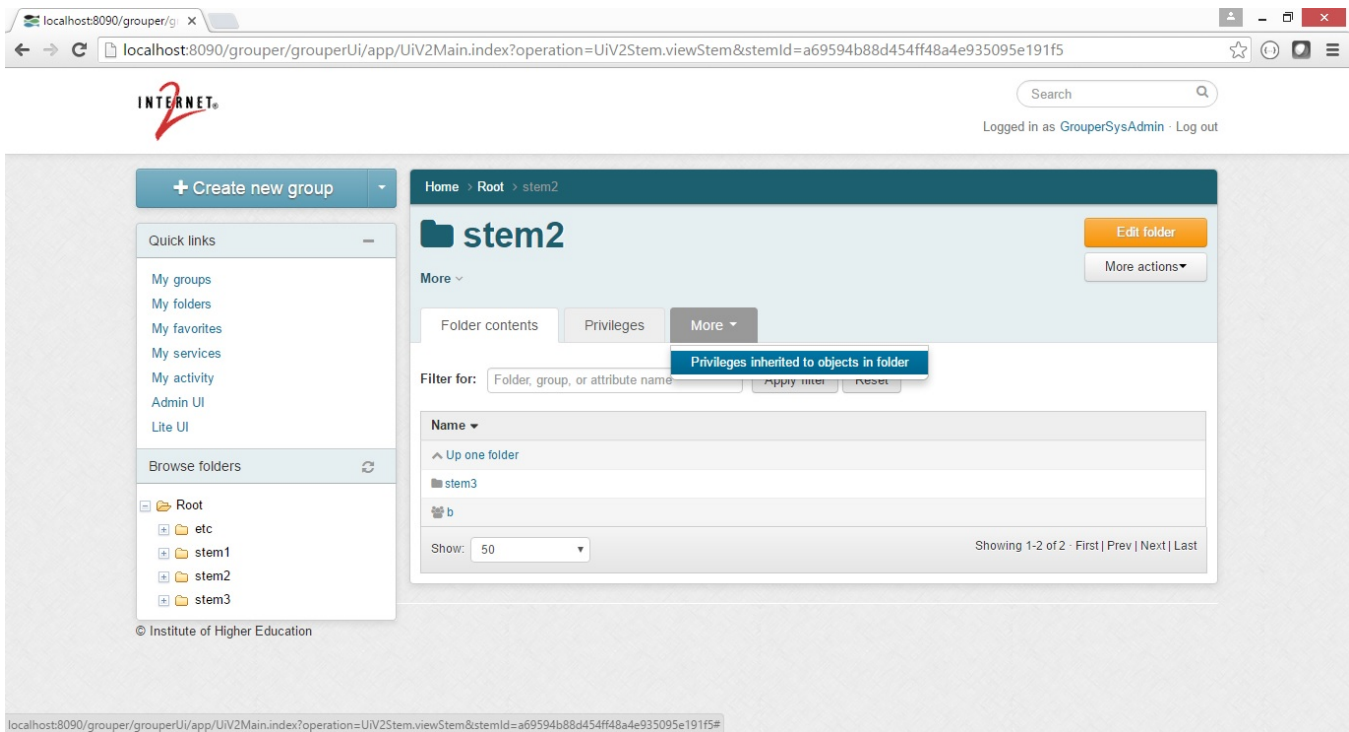
`grouper_v2_3_0_api_patch_90`
`grouper_v2_3_0_ui_patch_38`

These Jiras are implemented:

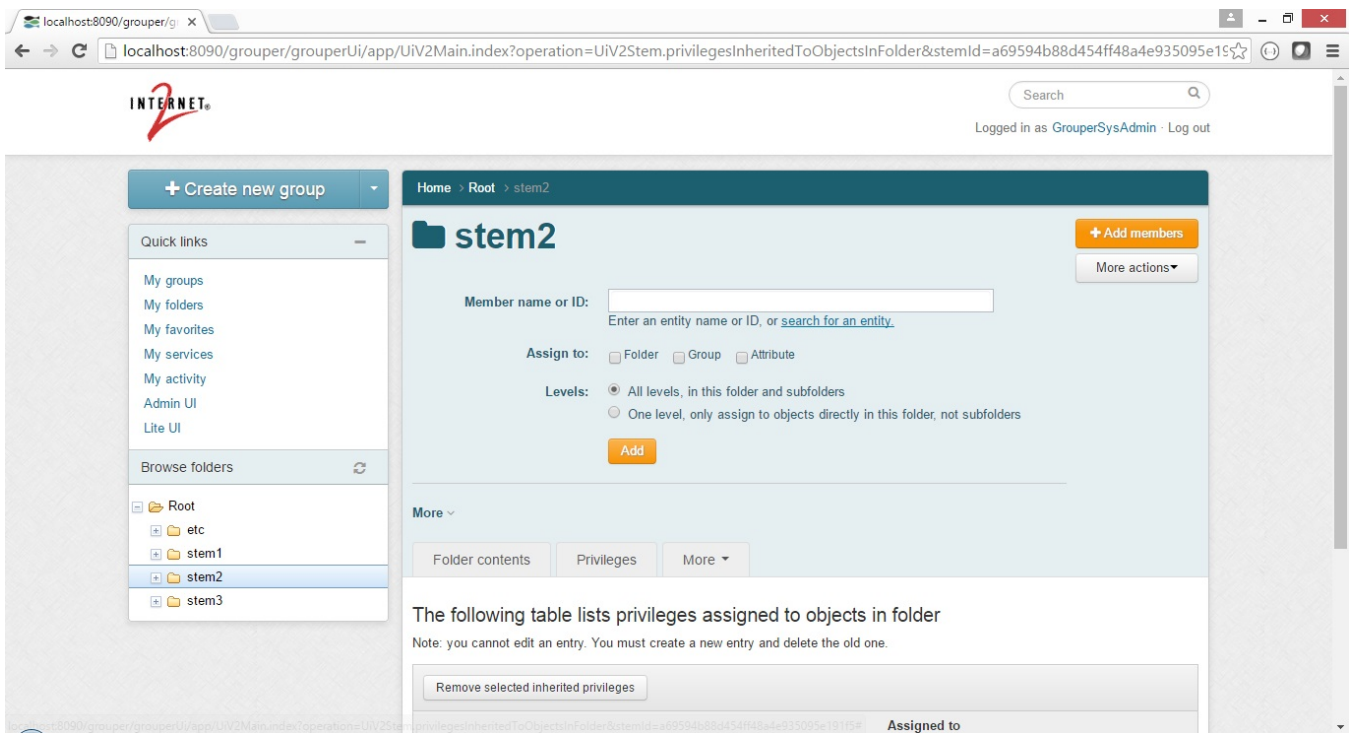
[GRP-1663: inherited privileges should revoke those privileges to subobjects](#)
[GRP-1664: do not add admin privileges to root or wheel when creating objects](#)
[GRP-1665: do not add admin privileges to inherited admins](#)
[GRP-1667: a folder inherited privilege should apply to the assigned folder](#)

Screen: View or assign inherited privileges in a folder

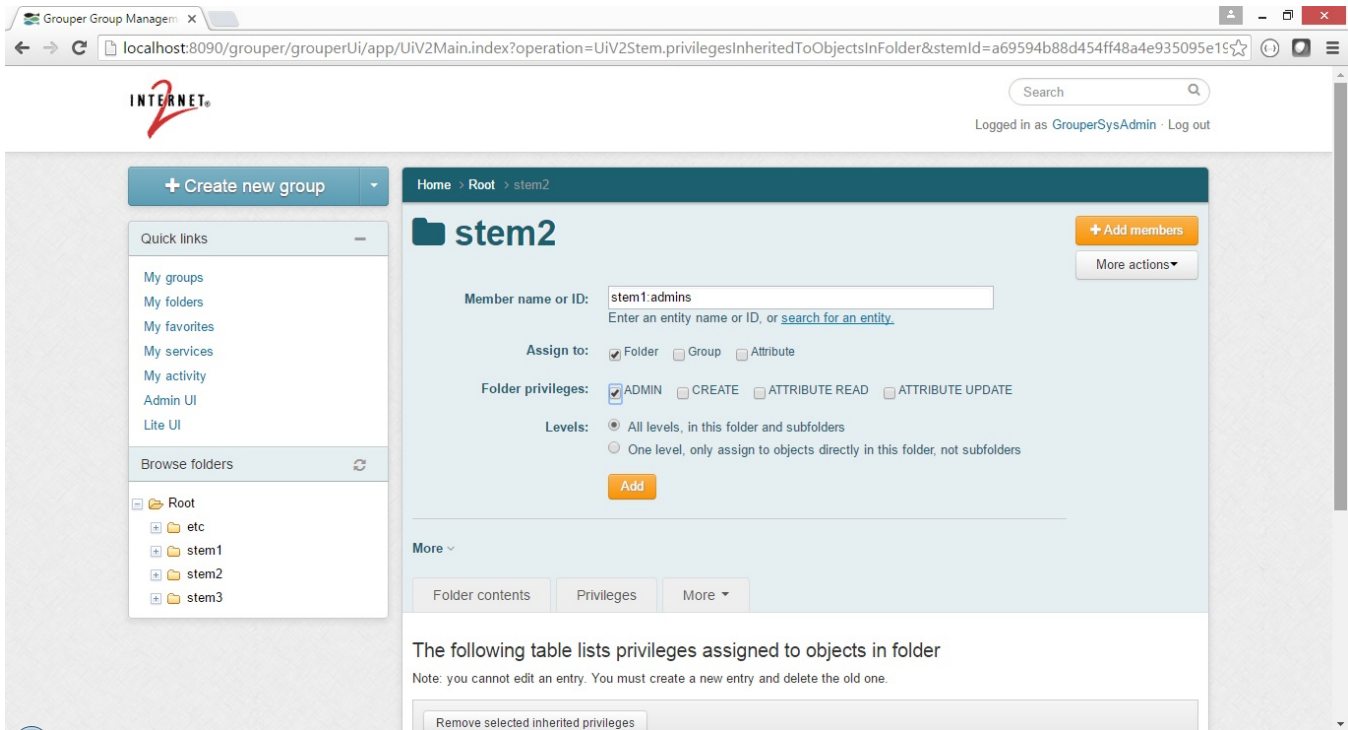
On a folder screen, if you are an ADMIN (and you can manage inherited privileges, see below), you can click "More -> Privileges inherited to objects in folder"



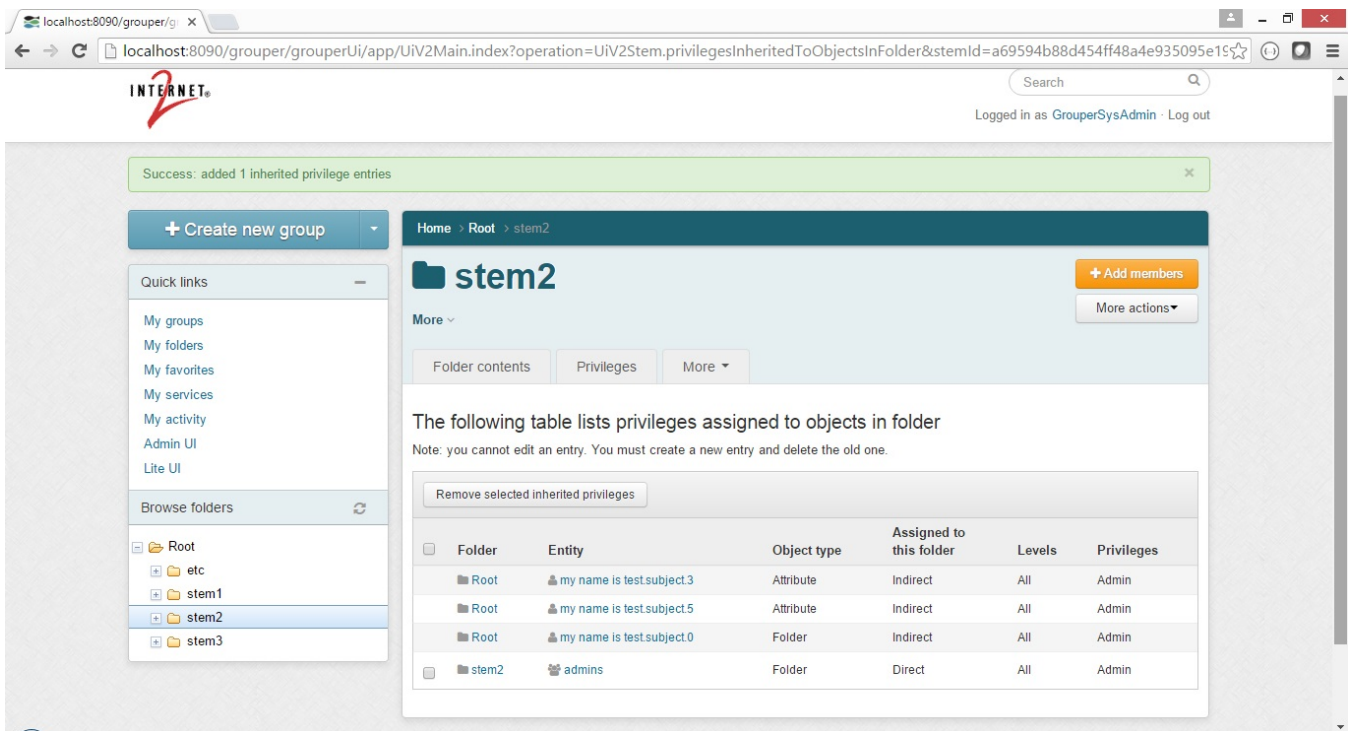
Click "Add members" to add a new inherited privilege



Select a member and the type to "Assign to" (which could be multiple types at once)



You can delete direct inherited privileges (which are assigned to this folder). To delete inherited indirect entries, click on that folder and delete from there



Screen: View inherited privileges that affect a group

If you are an ADMIN of a group and can view inherited privileges, pull a group up on the UI and click "More -> This group's privileges inherited from folders"

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.viewGroup&groupId=e4ecd8ff4cfa45c8a940ca0c1e6a384d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- admins
- stem2
- stem3

Home > Root > stem1 > admins

admins

+ Add members

More actions

Members Privileges More

The following table lists a

Filter for: All members

Remove selected members

Entity name Membership

my name is test.subject.0 Direct

Show: 50

Showing 1-1 of 1 · First | Prev | Next | Last

© Institute of Higher Education

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.viewGroup&groupId=e4ecd8ff4cfa45c8a940ca0c1e6a384d#

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.thisGroupsPrivilegesInheritedFromFolders&groupId=e4ecd8ff4cfa45c8a940ca0c1e6a384d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- admins
- stem2
- stem3

Home > Root > stem1 > admins

admins

More actions

Members Privileges More

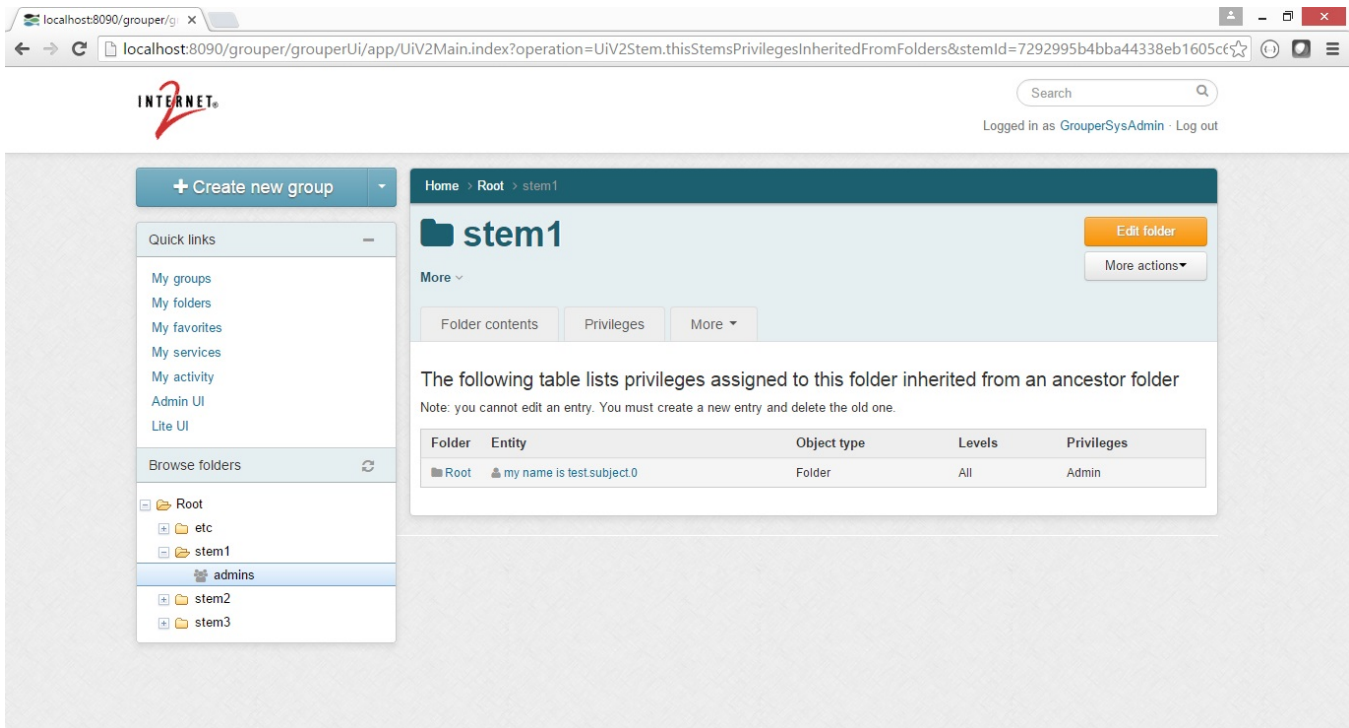
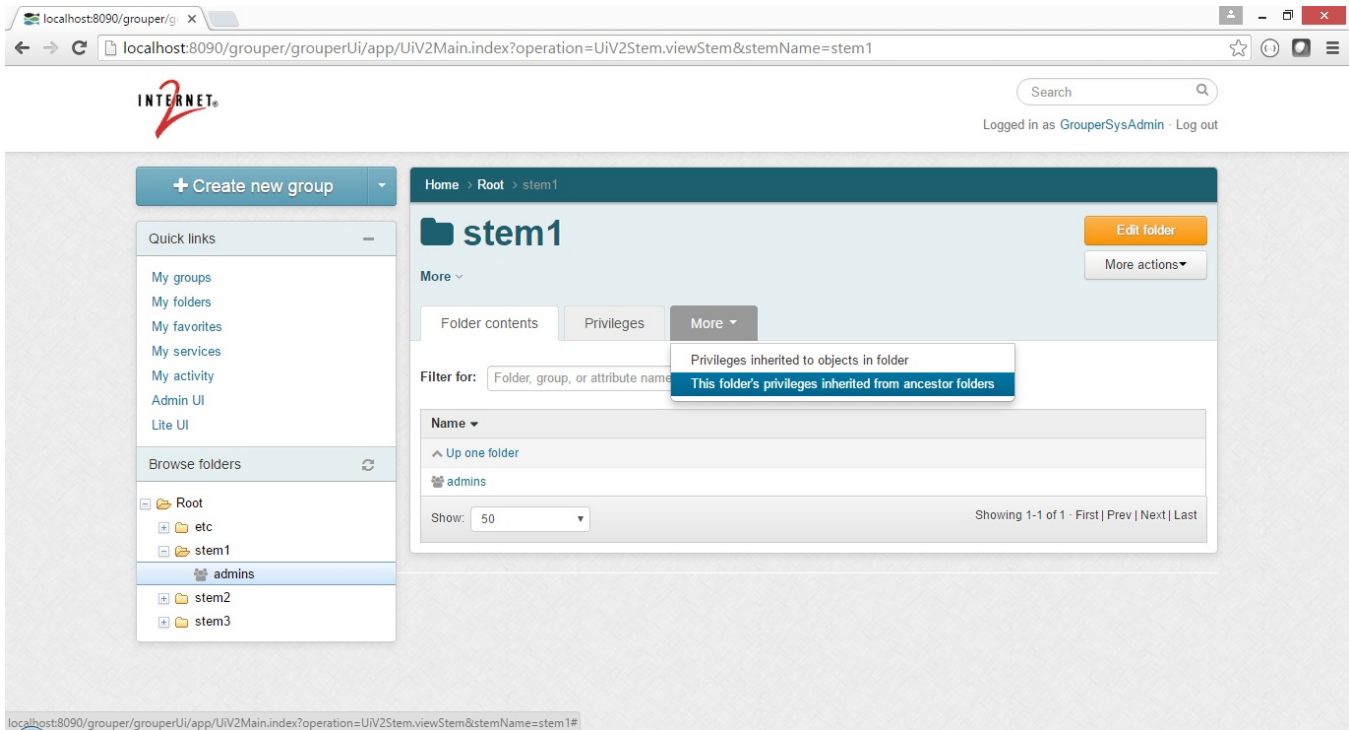
The following table lists privileges assigned to this group inherited from a folder

Note: you can create or delete inherited privileges in the folder screen.

Folder	Entity	Object type	Levels	Privileges
Root	my name is test.subject.7	Group	All	Read, View
stem1	my name is test.subject.6	Group	One	Update, Read

Screen: View inherited privileges that affect a folder

If you are an ADMIN of a folder and can view inherited privileges, pull a folder up on the UI and click "More -> This folder's privileges inherited from ancestor folders"



Screen: View inherited privileges that affect an attribute definition

If you are an ADMIN of an attribute definition and can view inherited privileges, pull an attribute definition up on the UI and click "More -> This attribute's privileges inherited from ancestor folders"

localhost:8090/grouper/g X

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2AttributeDef.viewAttributeDef&attributeDefId=6a8695149d954406ae56f5612db8d37d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- attribute
- attrExternalSubjectInvite
- externalSubjectInviteAttrDef
- externalSubjectInviteDef
- externalSubjectEmailAddress
- externalSubjectInvite
- externalSubjectInviteDate

Home > Root > etc > attribute > attrExternalSubjectInvite > externalSubjectInviteAttrDef

Attribute definition

externalSubjectInviteAttrDef

Edit attribute

More actions

More

Attribute names Privileges More

This attribute's privileges inherited from folders

The following table lists all attribute names associated with this attribute definition

Filter for: Attribute name Apply filter Reset

Delete selected attribute names

Folder	Attribute name	Actions
attrExternalSubjectInvite	externalSubjectEmailAddress	Actions
attrExternalSubjectInvite	externalSubjectInviteDate	Actions
attrExternalSubjectInvite	externalSubjectInviteEmail	Actions
attrExternalSubjectInvite	externalSubjectInviteEmailWhenRegistered	Actions

localhost:8090/grouper/g X

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2AttributeDef.thisAttributeDefsPrivilegesInheritedFromFolders&attributeDefId=6a8695149d954406ae56f5612db8d37d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- attribute
- attrExternalSubjectInvite
- externalSubjectInviteAttrDef
- externalSubjectInviteDef
- externalSubjectEmailAddress
- externalSubjectInvite
- externalSubjectInviteDate
- externalSubjectInviteEmail

Home > Root > etc > attribute > attrExternalSubjectInvite > externalSubjectInviteAttrDef

Attribute definition

externalSubjectInviteAttrDef

Edit attribute

More actions

More

Attribute names Privileges More

The following table lists privileges assigned to this attribute inherited from a folder

Note: you can create or delete inherited privileges in the folder screen.

Folder	Entity	Object type	Levels	Privileges
Root	my name is test.subject.3	Attribute	All	Admin
Root	my name is test.subject.5	Attribute	All	Admin
etc	my name is test.subject.8	Attribute	All	View, Read

Screen: View inherited privileges that affect a subject

If you can view inherited privileges, pull an entity up on the UI and click "More -> This subject's privileges inherited from folders"

localhost:8090/grouper/g x

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Subject.viewSubject&subjectId=test.subject.0&sourceId=jdbc

INTERNET®

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- stem2
- stem3

Home > my name is test.subject.0

my name is test.subject.0

+ Add to a group

Add to my favorites

Unique ID: test.subject.0

Email: test.subject.0@somewhere.someSchool.edu

Name: my name is test.subject.0

Description: description.test.subject.0

More

Memberships Group privileges Folder privileges Attribute privileges More

This subject's privileges inherited from folders

The following table lists all groups in which my name is test.subject.0 is a member.

Filter for: All groups Group name Apply filter Reset

Remove selected groups

Folder	Group name	Membership	
grouperUI	grouperUIUserData	Direct	Actions
stem1	admins	Direct	Actions

localhost:8090/grouper/g x

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Subject.thisSubjectsPrivilegesInheritedFromFolders&subjectId=test.subject.0&sourceId=jdbc

INTERNET®

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- stem2
- stem3

Home > my name is test.subject.0

my name is test.subject.0

+ Add to a group

Add to my favorites

Unique ID: test.subject.0

Email: test.subject.0@somewhere.someSchool.edu

Name: my name is test.subject.0

Description: description.test.subject.0

More

Memberships Group privileges Folder privileges Attribute privileges More

The following table lists inherited privileges assigned to this subject

Note: you can only see entries in folders where you are the admin of relevant objects

Folder	Entity	Object type	Levels	Privileges
Root	my name is test.subject.0	Folder	All	Admin
stem3	my name is test.subject.0	Group	All	Update

© Institute of Higher Education

Screen: View inherited privileges assigned to members of a group

This is similar to seeing privileges assigned to a subject. Its a little confusing. This is not the privileges of this group that are affected by inherited privileges.

If you can view inherited privileges, pull a group you can VIEW up on the UI and click "More -> This subject's privileges inherited from folders"

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.viewGroup&groupId=e4ecd8ff4cfa45c8a940ca0c1e6a384d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- admins
- stem2
- stem3
- b
- stem3

Home > Root > stem1 > admins

admins

+ Add members

More actions

Members Privileges More

The following table lists a

Filter for: All members

Remove selected members

Entity name Membership

my name is test.subject.0 Direct

Show: 50

Showing 1-1 of 1 · First | Prev | Next | Last

This group's memberships in other groups

This group's privileges in other groups

This group's privileges in folders

This group's privileges in attribute definitions

This group's privileges inherited from folders

Inherited privileges assigned to members of this group

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Group.inheritedPrivilegesAssignedToThisGroupFromFolders&groupId=e4ecd8ff4cfa45c8a940ca0c1e6a384d

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Admin UI
- Lite UI

Browse folders

- Root
- etc
- stem1
- admins
- stem2
- stem3
- b
- stem3

Home > Root > stem1 > admins

admins

More actions

Members Privileges More

The following table lists inherited privileges assigned to members of this group

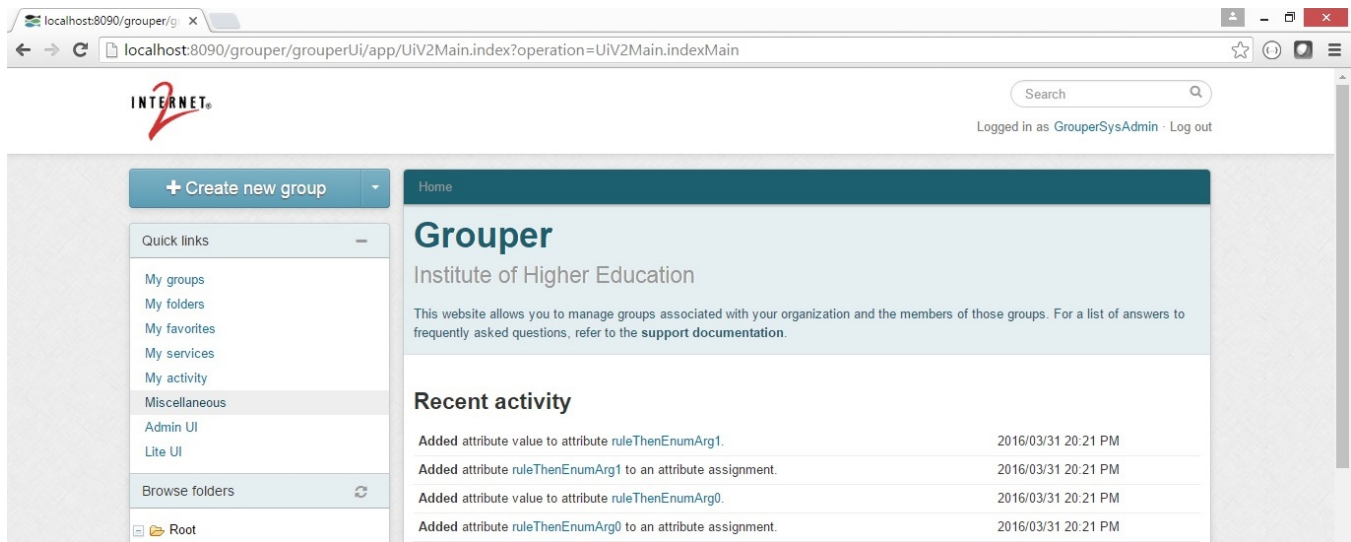
Note: you can only see entries in folders where you are the admin of relevant objects

Folder	Entity	Object type	Levels	Privileges
stem2	admins	Folder	All	Admin
stem3	admins	Attribute	All	View

Screen: View all inherited privileges in registry

View all inherited privileges in the registry that you are allowed to see.

Click on Miscellaneous (if you can see inherited privs you will see this link)



Click "Inherited privileges"

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Main.miscellaneous

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous
- Admin UI

Home > Miscellaneous

Miscellaneous

Functions across the repository

Inherited privileges

localhost:8090/grouper/g

localhost:8090/grouper/grouperUi/app/UiV2Main.index?operation=UiV2Main.globalInheritedPrivileges

INTERNET

Search

Logged in as GrouperSysAdmin · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous
- Admin UI
- Lite UI

Browse folders

- Root
 - etc
 - stem1
 - stem2
 - stem3

Home > Miscellaneous > Inherited privileges

Privileges inherited from folders

Note: you can only see entries in folders where you are the admin of relevant objects. You can create or delete inherited privileges in the folder screen.

Folder	Entity	Object type	Levels	Privileges
Root	my name is test.subject.3	Attribute	All	Admin
Root	my name is test.subject.5	Attribute	All	Admin
Root	my name is test.subject.7	Group	All	Read, View
Root	my name is test.subject.0	Folder	All	Admin
etc	my name is test.subject.8	Attribute	All	View, Read
stem1	my name is test.subject.6	Group	One	Update, Read
stem2	admins	Folder	All	Admin
stem3	admins	Attribute	All	View
stem3	my name is test.subject.0	Group	All	Update

© Institute of Higher Education

Privileges required to manage inherited privileges

This section describes who is allowed to view or assign inherited privileges.

In order to see rules configuration for inherited privileges on the UI, you need to be able to be an admin (stemAdmin) on a folder which is affected by the rule. If you want fewer people to be able to see the rule, you can adjust these in grouper.properties.

```
# require admin (GrouperSysAdmin or wheel group) to update inherited privileges
uiV2.privilegeInheritanceUpdateRequireAdmin = false

# require admin (GrouperSysAdmin or wheel group) to read inherited privileges
uiV2.privilegeInheritanceReadRequireAdmin = false

# require admin (GrouperSysAdmin or wheel group) to update inherited privileges
uiV2.privilegeInheritanceUpdateRequireGroup =

# require admin (GrouperSysAdmin or wheel group) to read inherited privileges
uiV2.privilegeInheritanceReadRequireGroup =
```

Note, you dont need to be able to read attributes on the assigned (parent or ancestor folder) to be able to see the privilege inheritance. You also do not need privileges on rule attributes. If you want to require rules attributes privileges set this in the grouper-ui.properties.

```
# if this is true you dont even need to be able to
uiV2.privilegeInheritanceDoesntRequireRulesPrivileges = false
```

If that is set to false, then to see the inherited privileges, you need to be able to READ the two attributeDefs for rules type and attributes

You can control the global screen (note, there is no paging as of 2.3.0)

```
# if show miscellaneous link
uiV2.showMiscellaneousLink = true

# if show global inherited privileges link
uiV2.showGlobalInheritedPrivilegesLink = true
```

sfd