

Do not allow someone to add themselves to a group

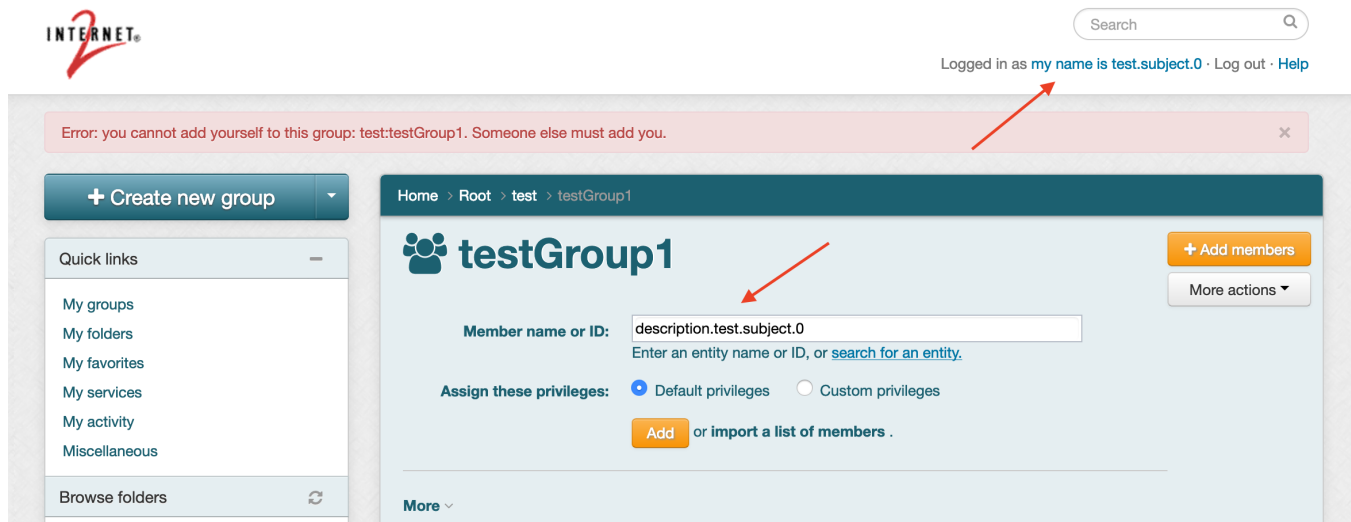
This is included in grouper 2.4 api patch 37, and 2.4 ui patch 18.

You can enforce separation of duties by not allowing a (updater/admin) user to add themselves to a group. Someone else has to.

By default a group admin can assign this to a group. But by default only wheel group members can unassign. This is configurable below. Group viewers can see if it is assigned (if this feature is enabled).

This is implemented with an implicit hook (you don't have to configure it)

Veto screen



View group screen

View if this feature is assigned to a group (viewers of group can see this in "more info")

Group

Home > Root > test > testGroup1

testGroup1

+ Add members

More actions ▾

Name:	testGroup1
Path:	test:testGroup1
ID path:	test:testGroup1
Alternate ID path:	
ID:	testGroup1
Created:	Fri Mar 15 12:58:37 AM EDT 2019
Creator:	GrouperSysAdmin
Last edited:	Fri Mar 15 12:58:37 AM EDT 2019
Last edited by:	GrouperSysAdmin
Type:	Group
Privileges assigned to everyone:	READ, VIEW
Composite owner:	This group is not a composite owner
Composite factor of other groups:	This group is not a direct composite factor of any other groups
ID index:	10008
UUID:	2e33375820a2455ead3b66fcb01c636d
Can add self:	No, updaters or admins cannot add themselves to this group

Less ^

Members

Privileges

More ▾

The following table lists all entities which are members of this group.

Edit if allowed to edit

testGroup1

Edit group

Group name:

Name is the label that identifies this group, and might change.

Group ID:

ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description:

Description contains notes about the group, which could include: what the group represents, why it was created, etc.

[Hide advanced properties ^](#)

Assign privileges to everyone: ☒ [READ](#) ☒ [VIEW](#) ☐ [OPTIN](#) ☐ [OPTOUT](#) ☐ [ATTRIBUTE READ](#)

Select which privileges should be public for everyone. This is the same as assigning a privilege to EveryEntity.

Type: ☒ Group
☐ Role

This could be a Group or a Role. A Group is a collection of entities. A Role is a Group which can also hold permission information centrally for the application.

Can add self:

If 'No', then this group has separation of duties where updaters/admins of the group cannot add themselves as a member. Someone else would need to add them.



Edit screen if not allowed to edit

testGroup1

Edit group

Group name:

Name is the label that identifies this group, and might change.

Group ID:

ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description:

Description contains notes about the group, which could include: what the group represents, why it was created, etc.

[Hide advanced properties](#) ^

Assign privileges to everyone:

☒ READ ☒ VIEW ☐ OPTIN ☐ OPTOUT ☐ ATTRIBUTE READ

Select which privileges should be public for everyone. This is the same as assigning a privilege to EveryEntity.

Type:

☒ Group
☐ Role

This could be a Group or a Role. A Group is a collection of entities. A Role is a Group which can also hold permission information centrally for the application.

Can add self:

No, updaters or admins cannot add themselves to this group
If 'No', then this group has separation of duties where updaters/admins of the group cannot add themselves as a member. Someone else would need to add them.

Save

Cancel

Configure

To enable this feature, in grouper.properties set this to true

```
# if you want a checkbox to not let users add themself to a group
# {valueType: "boolean"}
grouper.enable.rule.cannotAddSelfToGroup = true
```

Here are all the config options:

```

# if you want a checkbox to not let users add themself to a group
# {valueType: "boolean", requiresRestart="true"}
grouper.enable.rule.cannotAddSelfToGroup = false

# if you want group admins to be able to assign cannotAddSelf
# {valueType: "boolean"}
grouper.cannotAddSelfToGroup.allowAssignByGroupAdmins = true

# if group admins are not allowed to assign cannotAddSelf, then this group can, if blank then only Grouper
admins can assign
# {valueType: "string"}
grouper.cannotAddSelfToGroup.groupCanAssignByGroupAdmins = $$grouper.rootStemForBuiltinObjects$$:
cannotAddSelfToGroup:canAssignCannotAddSelf

# if you want group admins to be able to revoke cannotAddSelf
# {valueType: "boolean"}
grouper.cannotAddSelfToGroup.allowRevokeByGroupAdmins = false


# if group admins are not allowed to revoke cannotAddSelf, then this group can, if blank then only Grouper
admins can revoke
# {valueType: "string"}
grouper.cannotAddSelfToGroup.groupCanRevokeByGroupAdmins = $$grouper.rootStemForBuiltinObjects$$:
cannotAddSelfToGroup:canRevokeCannotAddSelf

```

Implementation

This is implemented as a single attribute assigned to a group

Home > Root > test > testGroup1




testGroup1
More actions ▾

More ▾

MembersPrivilegesMore ▾

Attribute assignments+ Assign attribute

The following table lists all attributes assigned to this group

Assignment type	Attribute name	Enabled?	Assignment values	Attribute definition	Choose action
Direct assignment	 cannotAddSelfAttributeDefName	enabled		 cannotAddSelfAttributeDef	Actions ▾