# Redmine - Defect #28264
## Global and public custom queries are shown as editable to non administrators in projects

2018-02-28 17:19 - Bernhard Rohloff

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Jean-Philippe Lang | **% Done:** | 0% |
| **Category:** | Issues | **Estimated time:** | 0.00 hour |
| **Target version:** | 4.0.0 | | |
| **Resolution:** | Fixed | **Affected version:** | 3.4.4 |

**Description**

If a globally available custom query is created by the administrator it gets shown as editable for project members who have the "Manage public queries" right. Because they don't have the right to edit a global public query, they get the following error message:

> *403 You are not authorized to access this page.*

... which I think is the intended behavior.

The exact issue is that the icons for edit and delete are incorrectly shown in the filter section.

**Steps to reproduce the issue:**

- Login as administrator
- Create a global and public query
- Login as project member with right "Manage public queries"
- Enter the "Issues" tab within a project
- Select the global and public query

**Expected result:** The icons for edit and delete are not shown

**Result:** The icons to edit and delete the query are shown in the filter section

The global "Issues" tab for all projects shows the expected result.

It seems to me that #14239 and #17669 describe the same issue but not in the correct way.

**Related issues:**

| | | |
|---|---|---|
| Related to Redmine - Defect # 17669: Non admin users can't modify public quer... | **Closed** | |
| Related to Redmine - Defect # 14239: Error 403 when trying to edit custom query | **Closed** | |
| Related to Redmine - Defect # 9108: Custom query not saving status filter | **Closed** | **2011-08-23** |

### Associated revisions

**Revision 17292 - 2018-04-08 15:23 - Jean-Philippe Lang**

Global and public custom queries are shown as editable to non administrators in projects (#28264).

**Revision 17384 - 2018-06-16 12:53 - Jean-Philippe Lang**

Fixed that "test_editable_by_for_global_query" and "test_editable_by_for_global_query_with_project_set" are identical (#28264).

## History

**#1 - 2018-02-28 22:37 - Marius BALTEANU**

*- Related to Defect #17669: Non admin users can't modify public queries for all project added*

**#2 - 2018-02-28 22:38 - Marius BALTEANU**

*- Related to Defect #14239: Error 403 when trying to edit custom query added*

**#3 - 2018-02-28 23:05 - Marius BALTEANU**

*- File fix_edit_delete_query_links_for_users_without_permissions.patch added*

*- File tests_for_28264.patch added*

*- Status changed from New to Confirmed*

@Bernhard, thanks for the detailed defect report.

I can confirm that the Edit / Delete links are shown even if the query is not editable by the respective user. This is confusing for the users.

I made 2 two tests to catch this issue:
- test_edit_global_public_query_should_not_be_allowed_for_non_admin_users which will pass in the current trunk and confirms that a non admin user doesn't has access to edit a public global query.
- test_index_with_global_public_query_id_for_should_not_show_edit_delete_links_for_non_admin_users which will fail because the links are rendered.

Also, I'm attaching a potential fix, but I'm not sure if is the correct solution because I don't know the reason behind overriding the @query.project in query_helper#retrieve_query.

**#4 - 2018-02-28 23:07 - Marius BALTEANU**

*- File deleted (tests_for_28264.patch)*

**#5 - 2018-02-28 23:07 - Marius BALTEANU**

*- File tests_for_28264.patch added*

**#6 - 2018-03-01 07:51 - Bernhard Rohloff**

Marius Thank you for confirming this issue.
I also dipped my toe into the code and the repository. I can confirm that the line you modify in your patch is the cause of that issue. You could also remove the entire line, which has the same effect as your attached conditional statement. The annotation of @queries_helper.rb reveals that this line (source:trunk/app/helpers/queries_helper.rb#L297) was introduced in r7656 to fix #9108.

Applying your patch (or removing the line, as I did) breaks the fix for #9108 and causes failing tests in issues_controller_test.rb.

I seems to me that overriding the queries project id in r7656 was a small and cheap hack to fight the symptoms but not the cause of the problem.
The actual problem of #9108 is the fact that the project id for the session is extracted from the query what doesn't work if the query is global and has no project.

So I think if we get #9108 properly fixed, the issue described here is solved, too.

**#7 - 2018-03-01 08:25 - Marius BALTEANU**

*- Related to Defect #9108: Custom query not saving status filter added*

**#8 - 2018-03-01 23:04 - Marius BALTEANU**

Bernhard Rohloff wrote:

> *Applying your patch (or removing the line, as I did) breaks the fix for #9108 and causes failing tests in issues_controller_test.rb.*

You're able to reproduce the issue from #9108 with the patch applied? I'm asking because I tried to follow the steps from the description and it worked as expected in both cases (global issues page and project issues page). Maybe I miss something.

I chose to add the condition instead of removing the entire line in order to change the behaviour only for global queries.

#### #9 - 2018-03-02 07:15 - Bernhard Rohloff

Marius BALTEANU wrote:

> *Bernhard Rohloff wrote:*
>
> > *Applying your patch (or removing the line, as I did) breaks the fix for #9108 and causes failing tests in issues_controller_test.rb.*
>
> *You're able to reproduce the issue from #9108 with the patch applied? I'm asking because I tried to follow the steps from the description and it worked as expected in both cases (global issues page and project issues page). Maybe I miss something.*

Oh I'm sorry! I mixed the issue numbers up... #9738 is the right one. #9108 was the issue linked with the last changeset the line was affected by. They reattached the line because they had a problem with breaking the fix of #9738, too.

> *I chose to add the condition instead of removing the entire line in order to change the behaviour only for global queries.*

As far as I could see, the project_id is stored within the queries table in the database and the queries are selected by the id of the current project. So there is no reason for overriding it with the same id except for the query is a global one.

#### #10 - 2018-03-03 13:37 - Marius BALTEANU

*- File deleted (fix_edit_delete_query_links_for_users_without_permissions.patch)*

#### #11 - 2018-03-03 14:27 - Marius BALTEANU

*- File fix_edit_delete_query_links_for_users_without_permissions.patch added*

I'm attaching an workaround which seems to work, but I'm not sure if is the proper fix. Maybe is better to add a new column (`is_for_all`) in the queries table with 0/1 values and update it using before_save hook (based on project_id value).

I've added Jean-Philippe Lang to this ticket, maybe he can take a look when he've time.

@Go Maeda, can I add this ticket to version:"3.3.7" or version:"4.0.0"? It'll be nice to fix it in the next version.

#### #12 - 2018-03-07 17:00 - Bernhard Rohloff

*- File fix_not_initialized_variable_in_query_model.patch added*

This bug caused me quite a headache but eventually I found the root of all evil in the query model.

The problem is that the overloaded initialize method doesn't get called.
Because of this the variable @is_for_all is not properly set and returns a false state in the condition statement.

I've fixed it now with the after_initialize callback method which seems to generally be the better way to do this, in reference to http://blog.dalethatcher.com/2008/03/rails-dont-override-initialize-on.html.

The attached patch is passing the tests in issues_controller_test.rb and query_controller_test.rb including the additional tests from Marius' patch.

#### #13 - 2018-03-07 22:16 - Marius BALTEANU

Bernhard Rohloff wrote:

> *This bug caused me quite a headache but eventually I found the root of all evil in the query model.*
> *The problem is that the overloaded initialize method doesn't get called.*
> *Because of this the variable @is_for_all is not properly set and returns a false state in the condition statement.*

Indeed, that was my conclusion too, but I wasn't be able to find a better solution than my workaround from the previous post.

> *I've fixed it now with the after_initialize callback method which seems to generally be the better way to do this, in reference to http://blog.dalethatcher.com/2008/03/rails-dont-override-initialize-on.html.*

Nice :) I didn't know about this callback. Today I learned something.

> *The attached patch is passing the tests in issues_controller_test.rb and query_controller_test.rb including the additional tests from Marius' patch.*

What do you think if you add to your patch the method is_for_all?? Something like:

```
def is_for_all?
  @is_for_all ||= project.nil?
end
```

and use this new method in the check instead of the @is_for_all variable.

Also, it looks like that you are using tabs instead of two spaces for indentation.

#### #14 - 2018-03-08 07:37 - Bernhard Rohloff

*- File fix_not_initialized_variable_in_query_model_V2.patch added*

Marius BALTEANU wrote:

> *What do you think if you add to your patch the method is_for_all?? Something like:*
> *[...]*
> *and use this new method in the check instead of the @is_for_all variable.*

Yep, that sounds good. I've implemented it in my new version of the patch and also gave it a more descriptive name.

> *Also, it looks like that you are using tabs instead of two spaces for indentation.*

Indeed, some tabs have crept into the patch. I've fixed them.

#### #15 - 2018-03-08 08:14 - Marius BALTEANU

Bernhard Rohloff wrote:

> *Yep, that sounds good. I've implemented it in my new version of the patch and also gave it a more descriptive name.*
>
> *Indeed, some tabs have crept into the patch. I've fixed them.*

Looks good now the patch to me.

#### #16 - 2018-03-08 08:31 - Marius BALTEANU

*- File deleted (fix_edit_delete_query_links_for_users_without_permissions.patch)*

#### #17 - 2018-03-21 10:05 - Go MAEDA

*- Target version set to 4.0.0*

The following patches look good to me. Setting target version to 4.0.0.

- attachment:fix_not_initialized_variable_in_query_model_V2.patch
- attachment:attachment:tests_for_28264.patch

Marius BALTEANU wrote:

> *@Go Maeda, can I add this ticket to version:"3.3.7" or version:"4.0.0"? It'll be nice to fix it in the next version.*

I think 4.0.0 is appropriate because the patch adds two new methods.

#### #18 - 2018-04-08 15:24 - Jean-Philippe Lang

*- Subject changed from Global and public custom queries are shown as editable to non administrators in projects. to Global and public custom queries are shown as editable to non administrators in projects*
*- Status changed from Confirmed to Closed*
*- Assignee set to Jean-Philippe Lang*
*- Resolution set to Fixed*

Fixed by using a slightly different fix in r17292 with test included.
Thanks for pointing this out.

#### #19 - 2018-04-29 07:29 - Marius BALTEANU

*- Status changed from Closed to Reopened*

Jean-Philippe Lang, looking at the fix committed, I'm observing that the tests "test_editable_by_for_global_query" and "test_editable_by_for_global_query_with_project_set" are identical. Is this ok?

#### #20 - 2018-06-16 12:54 - Jean-Philippe Lang

*- Status changed from Reopened to Closed*

Marius BALTEANU wrote:

> *Jean-Philippe Lang, looking at the fix committed, I'm observing that the tests "test_editable_by_for_global_query" and "test_editable_by_for_global_query_with_project_set" are identical. Is this ok?*

Fixed, thanks!

### Files

| | | | |
|---|---|---|---|
| tests_for_28264.patch | 1.56 KB | 2018-02-28 | Marius BALTEANU |
| fix_not_initialized_variable_in_query_model.patch | 827 Bytes | 2018-03-07 | Bernhard Rohloff |
| fix_not_initialized_variable_in_query_model_V2.patch | 1.43 KB | 2018-03-08 | Bernhard Rohloff |