Redmine - Defect #7773

Only Redmine administrators can get users from REST API

2011-03-04 08:25 - Jack T

Status:	New	**Start date:**	2011-03-04
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

On Redmine 1.1, only a user logged in as a Redmine administrator can get a list of users. Regular users get a HTTP 403 Forbidden error.

Getting a list of users is required in order to create an issue using the REST API and assign it to a project member.

Related issues:

Related to Redmine - Patch #24051: As a non-admin user using API, I want to b...	**Resolved**
Has duplicate Redmine - Defect #19794: non Admins cannot list users through API	**Closed**

History

#1 - 2011-04-18 23:33 - Jakub Wolny

exactly - I have the same problem while creating my app, which uses REST API.
Is there any workaround about this?
Maybe some list of fields which user's fields are "public" and can be retrieved by API?

#2 - 2011-04-19 09:03 - Etienne Massip

- Target version set to Candidate for next major release

#3 - 2011-12-28 12:08 - Alex Last

This improvement would eliminate the need to "Admin" access for Task Adapter, which would be very good. IS it possible to implement this in v. 1.3.1?

#4 - 2012-01-12 01:53 - sinco miao

--

#5 - 2012-01-12 01:54 - sinco miao

--

#6 - 2012-05-04 00:26 - Jeffrey Clark

Something smells funny. The users index is restricted to administrator, but the individual entries are freely accessible (/users/1 , /users/2 ...).

I would expect for non-administrators the response to be a list of project members for projects which I have access. In addition, `/projects/wizbang/users.xml` seems like an appropriate route to add.

#7 - 2012-11-01 23:39 - alessio alessio

- % Done changed from 0 to 10

as soon as possible

#8 - 2013-07-11 14:52 - Benoit Duffez

What's the status of this? It's been 10% implemented for 8 months now, but it still is a missing feature in my opinion.

#9 - 2013-07-12 21:21 - Jean-Philippe Lang

Jeffrey Clark wrote:

> Something smells funny. The users index is restricted to administrator, but the individual entries are freely accessible (/users/1 , /users/2 ...).

Wrong. Individual entries are accessible to non-admin users only if the requested user is active and is a member of a visible project or has a visible activity. There's too much logic involved to send an entire list of users.

On the other side, an API for getting the project members seems much more reasonnable. If it's any help, I'd be happy to add it to 2.4.0.

#10 - 2013-07-12 21:28 - Jean-Philippe Lang

Actually, the members list was added to the API in r8798 (eg. /projects/wizbang/memberships.xml, see Rest_Memberships). It's only accessible to users who have the "manage members" permission. We can make it accessible to anyone who can view the project.

#11 - 2013-07-15 10:25 - Benoit Duffez

Well, the REST API access is not on par with standard HTTP access. Indeed, on my server I have a public project, on which registered users can add issues and comments. Registration is open (yet validated by hand), so basically anyone can add issues and comments without being marked as members of that project.

So on HTTP access (e.g. /issues/123), anyone (including anonymous access) can see the users name, avatar.
With REST access, this information is unavailable because the raw list of users is not public (and restricted to admins), and because the individual users that may add issues or comment are not members of that project.

#12 - 2013-07-15 23:14 - Jean-Philippe Lang

Benoit Duffez wrote:

> So on HTTP access (e.g. /issues/123), anyone (including anonymous access) can see the users name, avatar.

Try /issues/123.xml, you will see the user names as long as you are allowed to view this issue.

> With REST access, this information is unavailable because the raw list of users is not public (and restricted to admins), and because the individual users that may add issues or comment are not members of that project.

The issue view is not the users list. Using regular HTML access, only admins can view the users list. It works the same with the API.

#13 - 2013-07-15 23:19 - Benoit Duffez

That's right. I didn't exactly mentioned what was missing, it's in fact only the email address that can be used to generate the gravatar URL, which generates the avatar.
I think this is a sensitive info that can't be disclosed, so I'll have to deal without.

Thanks a lot for the reminder, and thank you for your time and kind support.

#14 - 2013-07-16 08:38 - Etienne Massip

- Target version deleted (Candidate for next major release)

- % Done changed from 10 to 0

#15 - 2013-07-18 17:19 - Benoit Duffez

I'm sorry it just popped into my mind, I didn't mention it the other day.

Jean-Philippe Lang wrote:

> Actually, the members list was added to the API in r8798 (eg. /projects/wizbang/memberships.xml, see Rest_Memberships). It's only accessible to users who have the "manage members" permission. We can make it accessible to anyone who can view the project.

This would be great, and it'd make sense. HTTP access provides the members list, the REST API returns HTTP 401.

#16 - 2013-10-10 16:35 - Benoit Duffez

Hi,
Acutally, I'd need this implementation. This would make users that have rights to see a project have the right to get the list of users that are members of that project.

Say that I'm logged as a user that can post an issue on a project but is not admin.
Via HTTP: GET /projects/what/issues/new => there's the "assign to" input field, that contains the list of users
Via REST: GET /projects/what/memberships.(json|xml)?key=abcd => empty

#17 - 2013-11-30 14:37 - Steffen Gebert

Yes, I agree with that and have also the need for synchronisation with other systems. Why should information that is available anonymously via HTML not be available via REST (not even for authenticated, non-admin users)?

#18 - 2014-02-19 16:55 - tycho luyben

Any progress on this issue? I'm using the API and now I need to give manage members perms to get the possible users in the project which I don't want to do? Making the /projects/1/memberships.json work for only listing would be the solution (and a simple one at that)?

#19 - 2014-03-14 15:39 - Rene Pilz

I also agree Tycho and Steffen.
Please make this issue available.

We are currently developing some small Java-Apps that should fetch data from Redmine (we are evaluating using Redmine as Time-Tracking-System). And there it is a *must* to match user-id and user-logon (which looks only beeing able using the /users.xml Rest API call.

Another point:
get /users/<id>.xml works even with an non-Administrator User.
So we have this workaround: for (i=0;i<10'000;i++) GET /users/$i.xml

Works and we also have a full user list.

> Therefore: getting /users.xml blocked as non-admin is a bug.

#20 - 2014-03-31 09:13 - Luis Escamilla

Jean-Philippe Lang wrote:

> On the other side, an API for getting the project members seems much more reasonnable. If it's any help, I'd be happy to add it to 2.4.0.

I think so. Can you add this new feature to the next version?

Thanks in advance.

#21 - 2014-04-22 11:46 - anil venkata

When a Non-admin user is added to a project with manager as role, this non-admin user(as he is manager now) can see and add users as members to the project. This is achieved through http(i.e UI).
/projects/p1/settings tab -> "members" window -> "New Member" with users and role

But the same thing is not possible trough REST api.

Non admin user, though he is a manager of a project, he can't get the users list through rest api
GET <ip>/users.xml is not working i.e rendering 403 error [:require_admin] rendered_or_redirected.

At present we are using admin token in our tool along with GET <ip>/users.xml REST api, so that non-admin user(project manger) can get the users list, which he wanted to add to the project. Can this be fixed, so that non-admin user can get users list through REST api(as this is already happening and not restricted in HTTP i.e UI)?

#22 - 2014-09-10 21:50 - Kostas Manios

Anil,

There is another workaround for getting all users, by adding them to a group and having your project manager as the owner of this group (see forum discussion http://www.redmine.org/boards/3/topics/28005?r=43940#message-43940).

However I am still not able to add the new member to my project (which you said you did). Can I ask which API you are using? If you are using C#, would you be so kind as to help me out?

#23 - 2015-05-10 09:16 - Jean-Philippe Lang

- Has duplicate Defect #19794: non Admins cannot list users through API added

#24 - 2016-06-29 19:06 - Jake Kemme

If you have access to your Redmine code base,

app/controllers/users_controller.rb can be modified as follows:

```
- before_filter :require_admin, :except => :show
+ before_filter :require_admin, :except => [:show, :index]
+ before_filter :require_admin_or_api_request, :only => :index
```

Perhaps this could be submitted as a patch since all users can be fetched by looping on /users/$i.xml, so the restriction of the users.xml API call adds

no extra security.

#25 - 2016-09-29 07:55 - Sébastien Aubry

I agree, this should be submitted as a patch: I have hundreds of users to retrieve in order to convert the user_id I get inside Issues to firstname/lastname, and I now have to make multiple calls to /users/$i.xml.
Thanks!

#26 - 2016-11-01 17:29 - Mitsuhiro Tanino

- File 0001-Enable-none-admin-users-to-get-users-list-from-REST-.patch added

Hi,

I attached a patch to fix the issue based on the proposal from Jake on comment #24.
This patch is for Redmine master branch.

Thanks,

#27 - 2016-11-22 15:57 - Anonymous

Extra information (duplicated ticket) : #24051

Holger Just wrote:

> When removing the admin requirement on UsersController#index, there need to be the User.visible scope added to the ActiveRecord query in order to only show users which are visible to the current user.
>
> Once this is fixed, I think it is a great idea to have a user listing available. With the now available role-based controls for the user visibility, this should work without negatively affecting privacy.

#28 - 2016-11-22 17:49 - Toshi MARUYAMA

- Related to Patch #24051: As a non-admin user using API, I want to be able to filter users by their username without getting forbidden exception added

Files

0001-Enable-none-admin-users-to-get-users-list-from-REST-.patch	936 Bytes	2016-11-01	Mitsuhiro Tanino