Redmine - Patch #29459

Add admin flag to users API

2018-08-29 16:41 - Holger Just

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:	4.0.0		

Description

Currently, it is not possible to distinguish admin users from "normal" users via the API. This patch adds the admin flag to the users API. The flag is added to the index action (visible only to admins) and on the show action to admins only.

Note that due to a peculiarity of the API builder, the field is only included in JSON responses if the value is true. For XML, it is included with true and false values respectively. With the JSON API, it is thus not possible to distinguish a list of non-admin users from a list of users without the permission to see the admin status.

Related issues:

Related to Redmine - Feature #29871: Add admin flag to REST Users API documen...	**New**

Associated revisions

Revision 17496 - 2018-09-20 16:54 - Go MAEDA

Expose the Admin flag on the users api to admin users (#29459).

Patch by Holger Just.

History

#1 - 2018-09-02 05:01 - Go MAEDA

- Target version changed from Candidate for next minor release to 4.1.0

#2 - 2018-09-02 05:32 - Go MAEDA

IMHO, it is better to remove '|| (User.current == @user)' from the patch. Non-admin users can know whether they are admin or not by accessing /users.(xml|json).

```
Index: app/views/users/show.api.rsb
===================================================================
--- app/views/users/show.api.rsb    (revision 17471)
+++ app/views/users/show.api.rsb    (working copy)
@@ -1,6 +1,7 @@
 api.user do
   api.id          @user.id
   api.login       @user.login if User.current.admin? || (User.current == @user)
+  api.admin       @user.admin? if User.current.admin? || (User.current == @user)
   api.firstname   @user.firstname
   api.lastname    @user.lastname
   api.mail        @user.mail if User.current.admin? || !@user.pref.hide_mail
```

When a non-admin user gets their information via XML API, the response contains an '<admin>' element and they can know that they are non-admin user by seeing the value. But when a non-admin user accesses JSON API, it is impossible to make sure that whether they are admin or not because the response does not have 'admin' key, as you already mentioned. The behavior and specification will be different between XML and JSON. I think it is confusing.

#3 - 2018-09-19 17:35 - Holger Just

Go MAEDA wrote:

> IMHO, it is better to remove '|| (User.current @user)' from the patch. Non-admin users can know whether they are admin or not by accessing /users.(xml|json).

Unfortunately, only admin users can access /users.(xml|json). The endpoint is not accessible to "normal" users at all. Even in the web UI, there is currently no possibility for a non-admin user to find which users have admin permissions. Thus, I think there is a general need for *any kind* of check to restrict this information to only authorized persons.

For the API, I think the most common use-case for this added flag is for an API client to find whether its given credentials grant them admin permissions. If we remove the check for || (User.current @user), this check will be sort-of possible still, since admin users will still return true in /users/current.(json|xml) here while non-admin users will not contain the field at all (both in JSON and XML). Deoending on the client, this might make it a bit awkward to distinguish between a true value and a missing tag, but could probably be made to work.

If we retain the check, for XML, we will have a true or false value in the output for the current user, making it more consistent here. It will still not include the field for other users.

JSON will still only include the field if the value is true (which I think is a bug in the API builder which should be fixed separately). However, I think JSON clients are usually better equipped to handle "fluid" responses than XML clients.

Thus, in the end, I still think that it might a bit more consistent to include the field for the current user (esp. if or when we get to fix this API builder issue), handling the field the same way as the other filtered user fields. But I don't want to fight over this. If you think it should be removed to only show the field to admin users in any case, I can live with that too.

In both cases, you the following rule holds:

- If the admin field is present and contains a true value, the user is an admin
- If you are querying users/current.(xml|json) and the admin field is missing or false, the current user is not an admin
- If you are querying a different user and the field is not included, you don't know anything.

#4 - 2018-09-20 16:55 - Go MAEDA

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Target version changed from 4.1.0 to 4.0.0

Committed. Thank you for sharing the patch.

#5 - 2018-09-20 17:19 - Holger Just

- Status changed from Closed to Reopened

- Assignee changed from Go MAEDA to Holger Just

Thank you for committing the patch.

I will update the REST Users API documentation page accordingly.

#6 - 2018-10-28 21:50 - Marius BĂLTEANU

- Status changed from Reopened to Closed

- Assignee changed from Holger Just to Go MAEDA

Holger Just wrote:

> Thank you for committing the patch.
>
> I will update the REST Users API documentation page accordingly.

I've created a new ticket to track the documentation update. Please see #29871.

#7 - 2018-10-28 21:50 - Marius BĂLTEANU

- Related to Feature #29871: Add admin flag to REST Users API documentation added

Files

0001-Expose-the-Admin-flag-on-the-users-api-to-admin-user.patch	2.35 KB	2018-08-29	Holger Just