

ステータス:	Closed	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	REST API_32	予定工数:	0.00時間
対象バージョン:	4.2.0_152	作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/11870	status_id:	5
category_id:	32	tracker_id:	1
version_id:	152	plus1:	0
issue_org_id:	11870	affected_version:	
author_id:	54664	closed_on:	
assigned_to_id:	332	affected_version_id:	
comments:	11		

説明

On Users collection, an administrator may delete its own account on Redmine, making it unusable.

Doing exploratory testing tasks with API REST I've accidentally deleted my own user on <http://ecastillac.m.redmine.org>, making the server unusable for me.

I've tried this script, provided Admin user had @id=2@ as shown in a previous execution:

```
#!/usr/bin/perl -w
```

```
use strict;
use warnings;
```

```
our ($VERSION) = '0.01'; # q$Revision$ =~ /(d+)/;
```

```
use Test::More;
use Data::Dump;
```

```
# -----
```

```
use Redmine::API;
```

```
my($API_Key, $BASE_URL) = do 'config';
```

```
my $api = Redmine::API->new( auth_key => $API_Key
                             , base_url => $BASE_URL
                             , trace => $ARGV[0] || 0);
```

```
my($res, $res1);
```

```
# -----
```

```
#$res = $api->users->x->all();
#ddx $res->body;
```

```
$res1 = $api->users->user->del( 2 );
ddx $res1->body;
```

journals

I don't get why it would be a defect? Just don't delete your admin account if you have only one...

The web UI does not allow admins to delete your account unconditionally.

- "Administration > Users" page always disallows users to delete their own account
- Users can delete their own account on My account page when the setting "Allow users to delete their own account" is enabled, but admins are allowed to delete their own account on the page only when there is another user with an admin privilege

So, I think API should not allow avoiding the limitations. The following code disallows admins to delete their own accounts via API or by sending a crafted request if "Allow users to delete their own account" is not enabled.

```
diff --git a/app/controllers/users_controller.rb b/app/controllers/users_controller.rb
index 2fb297874..578ac5a9a 100644
--- a/app/controllers/users_controller.rb
+++ b/app/controllers/users_controller.rb
@@ -184,6 +184,8 @@ class UsersController < ApplicationController
   end

   def destroy
+    raise Unauthorized if @user == User.current && !@user.own_account_deletable?
+
     @user.destroy
     respond_to do |format|
       format.html { redirect_back_or_default(users_path) }
```

I've attached a patch based on #11870#note-2.

It was developed by pair programming with "@kfischer_okarin":

<https://www.redmine.org/users/204091>.

LGTM.

If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with @render_api_errors@ or something, but anyway it looks good to me.

Setting the target version to 4.2.0.

vzvu 3k6k wrote:

LGTM.

If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with @render_api_errors@ or something, but anyway it looks good to me.

Thank you for your feedback.

I changed to return error message.

@@user.own_account_deletable?@ will be false if User.current was the last admin user. If there is an opinion that it is better to display another error message only in that case, I will improve the patch

Mizuki ISHIKAWA wrote:

vzvu 3k6k wrote:

LGTM.

If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with @render_api_errors@ or something, but anyway it looks good to me.

Thank you for your feedback.

I changed to return error message.

I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

Go MAEDA wrote:

I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

Thanks for reviewing this patch!

Although there is no precedent that directly uses `render_api_errors` to return error messages, it is common to return validation error messages with `render_validation_errors`.

I don't think the behavior of the API from the user's perspective is that special.

And, in the case of exceptions that meet special conditions like this time, it is better to issue an error message even if it is different from other API responses.

I wrote it as above, but if the current specification makes it difficult to commit, I think it is better to prioritize the commit of the first patch!

I think for now it might be good to follow Redmine's current practice, i.e. no special error message.

But still it would be good to create another ticket (if one doesn't exist yet) to discuss/improve the general Rest API error response format of Redmine and adapt it to best practices for Rest APIs

Go MAEDA wrote:

I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

Thank you for pointing it out.

Certainly most of (or all of?) Redmine APIs don't return error messages when deletion fails. I think it is because in most cases users can easily guess why their request failed. On the flip side, it might be worth returning an error message when it is difficult for users to guess why.

Maybe this should be discussed on another issue as Kevin Fischer says.

Mizuki ISHIKAWA wrote:

`@@user.own_account_deletable?@` will be false if `User.current` was the last admin user. If there is an opinion that it is better to display another error message only in that case, I will improve the patch

I'm sorry for the late reply. Good catch, and thank you for writing another patch. I didn't think of it until you said.

As you suggest, I feel the message of "This user is your own user and cannot be deleted" can be confusing when the error reason is that `@User.current@` was the last admin user.

I've attached another patch to try to solve this confusion by adding another error message, though I'm not sure this API should return an error message for now.

Committed attachment:fix-11870.patch. Thank you for your contribution.

The following issues have been fixed in r20782:

- Users can delete their own account even when the setting "Allow users to delete their own account" is disabled
- An admin can delete their own account even if they are the last admin

履歴

#1 - 2022/05/10 17:15 - Admin Redmine

- カテゴリ を REST API_32 にセット

- 対象バージョン を 4.2.0_152 にセット