# Redmine - Defect #4825
## Several related bugs relating to registration, sign in and account preferences.

2010-02-13 03:25 - oliver stieber

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 2010-02-13 |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | Accounts / authentication | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | | **Affected version:** | |

**Description**

Hi, these bugs / feature requests which I consider to be more none crash bug like are fairly well related and all relate to the same activity which I was trying to perform so I've filed them as one bug report  but you will probably want to split them up in to several and relate them together as desired.

went to register (http://www.redmine.org/account/register)and got the following message when I posted the form
'Invalid form authenticity token.'

Thought this may be because I was already registered so went to sign in (http://www.redmine.org/login)got the following message

'Invalid form authenticity token.'

Thought the problem may be because I was using Konqueror so tried firefox.

clicked on submit once, didn't appear to do anything just reloaded register page

clicked on submit again

This time got the message 'Login has already been taken'

So went to sign in, put in exactly the same Username and password I did in the register page and signed in ok.

updated my email address (I used my work email address when I first registered and no longer work there)

clicked on sae and firefox (Mozilla Firefox 3.5.7, Copyright (c) 1998 - 2009 mozilla.org) closed (no error message /crash message either in X or on the terminal `I started firefox fro mthe terminal`)

If the credentials entered in the register page the register page should
a: log you in and tell you that you already had an account.
b: update any information that is now different,
prohaps it should firstly ask you if you name has changed reciently if the firstname and lastname no longer match.
and ask you if you may have changed your email address latley too if the email address doesn't match, if the first name and last name matched the existing registration it may be an idea to display the old email address and ask the user which one they want to use.

There's an option to remember / remain logged in, there should really be an associated list of options (drop down box etc...) so that the user can select to just rememberthe user name, lock to this ip, make persistant till midnight, for a day, for a week, forever, until the sign out, untill they close the browser  etc.. There should also be a way of stopping it being remembered without the user having to delete cookies (this is especially required since firefox 'stupidly' now blocks sites when you remove cookies from them without prompting which makes it a pain in the arse to get cookies working again and user who don't know about things like that may never figure out what going on and why the redmine site no longer works.

Also, the user account preferences should have an option to return to the last page viewed etc... when they next login or if they are

automatically logged in. This is really handy and very desireable if the reason they left the redmin site is because the browser crashed or the power went etc....

**Related issues:**

| | | |
|---|---|---|
| Related to Redmine - Defect # 5230: Invalid form authenticity token. | **New** | **2010-04-01** |
| Related to Redmine - Defect # 5915: Invalid form authenticity token for some ... | **Closed** | **2010-07-20** |
| Related to Redmine - Defect # 9239:  autenticity_token is not checked properly | **Closed** | **2011-09-13** |

## History

#### #1 - 2010-06-19 20:25 - Greg Mefford

The first problem sounds like something funny going on in the browser. The authenticity token makes sure that you are submitting back data for a form that you just asked for, and that no one else already submitted data for that form. That's why it worked later when you tried again fresh.
This suspicion is confirmed by the browser crashing; it seems extremely unlikely that a bug in Redmine would crash Firefox unless something else was amiss.

#### #2 - 2010-10-07 05:40 - Ewan Makepeace

I am cross posting this from #5230 as it seems related:
---
This is a huge problem for me and is very simple to reproduce:

1. Log out from Redmine.
2. Go to your email
3. Click on the links on three different issues in your email so that three tabs open in your favourite browser.
4. Presumably each is prepopulated with your login details in the browser.
5. On teh first tab you can click login and be redirected to the issue.
6. On the other tabs when you hit login you get the dreaded "Invalid form authenticity token.". Now you have to login again and after you do so your redirect is lost so you close the tab and go and look for the email again.

I hate this message so much I am considering moving off Redmine (Pivot Tracker looks rather attractive?). Seriously this is a monster issue that is driving me insane.
---
Redmine seems to be using a much more restrictive security token system than other authenticated sites I use (where I can typically login multiple times without complaint) and is as a significantly broken by my standards.
PS Redmine 1.0.1.devel.4167 (MySQL)

#### #3 - 2011-04-18 18:28 - Florent Viard

Hi,

This problem is also the same as the one of the bug: http://www.redmine.org/issues/5915 i think.
I was annoyed by this bug for a long time and finally discovered the source of it.
Some browsers (mainly chrome, but also firefox) have something called an Autofill function to autocomplete form fields like the login and password boxes. But, stupidly, they also keep in memory the content of the hidden fields.

That's why the authenticity token used for the first login is used for the following try to login.

A solution to this problem, is to add the following input attribute to the "authenticity_token" hidden input field in the login page:
autocomplete="off"

Thus, browsers will stop to try to autocomplete this field automatically :)

#### #4 - 2011-06-27 15:41 - Joel Nothman

The authenticity token is generated each time the login page is loaded. This is a huge problem for people who load multiple tabs in their browser.
I.e. if I have three URLs (url1, url2, url3 that require login, and have them on the list of pages to open when I open a new browser session, I will land up at:

1. http://redmine/login?back_url=url1
2. http://redmine/login?back_url=url2
3. http://redmine/login?back_url=url3

Each will have its own authenticity_token, invalidating the previous one served (but the user doesn't care which order the server serves, just as Redmine shouldn't care what order the user opens pages, and whether they are simultaneously accessed).
Further, if the user has provided credentials and successfully authenticated in window #1, both of the following will fail to get the user to url2 in window #2:

- reloading the page (will open login, rather than following back_url)
- entering login credentials again (will report invalid authenticity token, rather than followign back_url)

I think there are 3 bugs here:

- If a signed in user opens the login page and a back_url is provided, redirect to the back_url
- If login fails (due to invalid authenticity token or otherwise), but the user is already signed in, and back_url is provided, redirect to the back_url
- Remove the need for an authenticity_token for login