Redmine - Feature #1763
Autologin-cookie should be configurable

2008-08-11 03:55 - Mischa The Evil

Status:	Closed	**Start date:**	2008-08-11
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	1.2.0		
Resolution:	Fixed		

Description

Currently the autologin-cookie is generated by *./app/controllers/account_controller.rb*. There are currently no configurable settings regarding the autologin-cookie.

These facts currently makes the autologin-functionality unusable when using multiple (seperate) Redmine deployments on one domain under different sub-URI's. It may also interfere with autologin-cookies from other installed apps under the different sub-URI's.

It's possible to hack the account_controller manually in such a way that those properties are getting set for the cookie but than "it" looks like it breaks something, since after such hack the cookie isn't deleted anylonger when the user logs-out. This is possibly caused by the fact that the cookie with such extended properties doesn't match the search-string when the logout-routines are triggered and run (though I'm not sure about that).
I'd propose to make the following properties configurable (or add them) for the autologin-cookie:

1. key
2. path
3. secure

(3) is equal to the request in #982 but I thought it was better to list it here also.

Furthermore issue #540 is related too this issue too, since it mentions the in this issue described behaviour also.

Related issues:

Related to Redmine - Feature # 7408: Add an application configuration file	**Closed**	**2011-01-22**
Related to Redmine - Feature # 540: Append suffix to cookie name	**Closed**	
Related to Redmine - Feature # 982: option to set secure flag on session and ...	**New**	**2008-04-03**

Associated revisions

Revision 4756 - 2011-01-23 12:20 - Jean-Philippe Lang

Makes the autologin cookie configurable (#1763).

The cookie attributes (name, path, secure) can now be set in config/configuration.yml.

History

#1 - 2010-09-23 12:06 - Boris Pigeot

Cookie secure should be set if we use "https" option on the admin page.

For now :

curl -vv -I https://a_redmine_install/subdirectory_of_redmine/

set a "wrong" cookie path :

Set-Cookie:

_redmine_session=BAh7BjoPc2Vzc2lvbl9pZCIlZTFhMjU5ODJiZmViNDI1Y2E5OWU1Y2VjM2VmODg1Njk%3D--3fe3555b3d342f669f4df45d66b7d23f4e9a6b7d23f4e9a6b86; path=/; HttpOnly

path should be /redmine/
and the cookie should be secure.

#2 - 2010-09-23 13:23 - Felix Schäfer

- Status changed from New to Closed
- Resolution set to Invalid

You can set all these things as you desire in the config/initializers/session_store.rb, mine says:

```
# This file was generated by 'rake config/initializers/session_store.rb',
# and should not be made visible to public.
# If you have a load-balancing Redmine cluster, you will need to use the
# same version of this file on each machine. And be sure to restart your
# server when you modify this file.

# Your secret key for verifying cookie session data integrity. If you
# change this key, all old sessions will become invalid! Make sure the
# secret is at least 30 characters and all random, no regular words or
# you'll be exposed to dictionary attacks.
ActionController::Base.session = {
  :session_key => '_redmine_session',
  #
  # Uncomment and edit the :session_path below if are hosting your Redmine
  # at a suburi and don't want the top level path to access the cookies
  #
  # See: http://www.redmine.org/issues/3968
  #
  # :session_path => '/url_path_to/your/redmine/',
  :secret => '<edited-key>'
}
```

So the sub-uri and the distributed setup points are addressed in the comments, you can still set the :secure option by hand if you need, but the cookies are encrypted and signed, I doubt anyone could read or change them to anything meaningful if your :secret is long enough.

As to making any of these options DB-driven: it won't work because you'd have to already have a working config to get to the administration page to set them, it would add complexity and DB-calls to the startup, and I'm not even sure you could call the DB at the point where this stuff needs to get set.

Closing this as invalid because I don't see the feasibility of this, nor the motivation as it is already taken care in the docs of the proper files.

#3 - 2010-09-26 13:25 - Boris Pigeot

Thanks for your return.
In this case, maybe a commented :
:secure => true,
could be a nice idea.
Here is my new session_store.rb :

```
ActionController::Base.session = {
  :session_key => 'dev_',
```

```
    :session_path => '/redmine/',
    :domain => 'my_domain',
    :secure => true,
    :secret => 'c8a8df481...'
  }
```

Some doc about memcache stored session (and cache) could be great.

I just discover ruby and redmine.

#4 - 2010-12-17 06:43 - Mischa The Evil

- Status changed from Closed to Reopened

- Resolution deleted (Invalid)

Felix Schäfer wrote:

> *You can set all these things as you desire in the config/initializers/session_store.rb, mine says:*
>
> *[...]*
>
> *So the sub-uri and the distributed setup points are addressed in the comments, you can still set the :secure option by hand if you need, but the cookies are encrypted and signed, I doubt anyone could read or change them to anything meaningful if your :secret is long enough.*

That true... For the session cookie.... But I opened this issue specifically for the autologin cookie which is not yet configurable IMHO.

#5 - 2011-01-23 13:23 - Jean-Philippe Lang

- Status changed from Reopened to Closed

- Target version set to 1.2.0

- Resolution set to Fixed

r4756 makes the autologin cookie configurable in the application configuration file (see #7408).