Redmine - Feature #3920

REST API for authentication

2009-09-25 02:07 - Eric Davis

Status:	Closed	**Start date:**	2009-09-25
Priority:	Normal	**Due date:**	
Assignee:	Eric Davis	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.0		
Resolution:	Fixed		

Description

As part of the REST API (#296), there should be a way to authenticating users. I'm planning to implement a few different ways to authenticate for the API:

- HTTP Basic Authentication - http://username:password@www.redmine.org/issues
- HTTP Basic Authentication with an API token, similar to the Atom feeds - http://AB458D45B2:X@www.redmine.org/issues
- API token via the url parameters - http://www.redmine.org/issues?api_key=AB458D45B2

Thoughts? Additional ideas?

Related issues:

Blocks Redmine - Feature #1214: REST API for Issues	**Closed**	**2008-05-08**
Blocks Redmine - Feature #296: REST API	**Closed**	

Associated revisions

Revision 3217 - 2009-12-23 07:27 - Eric Davis

Added an API token for each User to use when making API requests. (#3920)

The API key will be displayed on My Account page with a link to reset or generate a new one. All existing users will have a token generated by the migration.

Revision 3218 - 2009-12-23 07:27 - Eric Davis

Allow authenticating with an API token via XML or JSON. (#3920)

Revision 3219 - 2009-12-23 07:27 - Eric Davis

Added support for HTTP Basic access to the API. (#3920)

A user can authenticate using either their:

- username/password
- api-key/random

Revision 3220 - 2009-12-23 07:27 - Eric Davis

Added an Admin setting to enable/disable the REST web service. (#3920)

History

#1 - 2009-11-01 17:21 - Katsunori Kanda

Hello,
how about WSSE that is used with some popular web services like Flickr do you think? I think it's better choice, if you assume the connection without ssl.

And also I found a good article about http authentication: HTTP Authentication and Feed Security

#2 - 2009-11-02 16:54 - Holger Winkelmann

what about API login returns a session token which will be used by further requests ?

#3 - 2009-11-04 02:33 - Katsunori Kanda

Holger Winkelmann wrote:

> what about API login returns a session token which will be used by further requests ?

We can choose the suitable way like using cookie or request parameters as same as the normal web applications do, but we must decide whether our API is stateless or not. This dicision is indipendent of choosing the way of authentication.

BTW, I make a mistake. I wrote Flick API used WSSE, but it didn't use. Flickr API authentication is original.

#4 - 2009-12-15 11:47 - Pierre Gambarotto

Eric Davis wrote:

- HTTP Basic Authentication with an API token, similar to the Atom feeds - http://AB458D45B2:X@www.redmine.org/issues

this one has my preference. This way you can distribute an access without giving away your favorite password.

This implies for an authenticated user a way to (re)generate a token. It should be on the account page.

#5 - 2009-12-20 21:34 - Eric Davis

Holger Winkelmann wrote:

> what about API login returns a session token which will be used by further requests ?

I don't like that approach. It would require the server to keep the state of the requests and with the latest Redmine, sessions are stored on the client (encrypted cookies).

Pierre Gambarotto wrote:

> This implies for an authenticated user a way to (re)generate a token. It should be on the account page.

Correct.

#6 - 2009-12-21 02:35 - Eric Davis

- % Done changed from 0 to 50

I've got the token part of this implemented in a private branch. With it, users will have an API token they can use to access Redmine just like a login. I've tested it on the News module and it's working properly for both XML and JSON formats (News already accepts key authentications for the atom feed so it wasn't difficult to add new formats).

curl http://localhost:3000/news.xml?key=01fc3e3832e32ae8c12bf0c3b0819ca4a5972825

```
<?xml version="1.0" encoding="UTF-8"?>
<news type="array">
  <news>
    <author-id type="integer">1</author-id>
    <comments-count type="integer">0</comments-count>
    <created-on type="datetime">2009-12-20T16:31:09-08:00</created-on>
    <description>testttsstst</description>
    <id type="integer">1</id>
    <project-id type="integer">36</project-id>
    <summary></summary>
    <title>Test</title>
  </news>
</news>
```

curl http://localhost:3000/news.json?key=01fc3e3832e32ae8c12bf0c3b0819ca4a5972825

```
[{"title":"Test","created_on":"2009/12/20 16:31:09 -0800","project_id":36,"id":1,"summary":"","description":"t
estttsstst","comments_count":0,"author_id":1}]
```

I'm not sure if the HTTP Basic authentication will be able to work transparently. Would it be a worthwhile addition or should I just stick with the key option like the rest of Redmine? (e.g. ATOM feeds, reposman.rb) I can always add the HTTP Basic in later if someone can help find an easy way to add it.

#7 - 2009-12-21 03:01 - Eric Davis

Nevermind, we will need HTTP Basic if we want to work with ActiveResource.

#8 - 2009-12-23 07:28 - Eric Davis

- Status changed from 7 to Closed

- % Done changed from 50 to 100

- Resolution set to Fixed

This should be considered experimental until further testing.

I added a REST API for authentication with support for three styles of sending the credentials:

- Key parameter - each user has an API token they can manage like the RSS tokens.
- Username and password via HTTP Basic
- Key via HTTP Basic

I'll document how to use the API later, but here are some example calls to my server running on port 3000 at "localhost"

```
# Key parameter
curl http://localhost:3000/news.xml?key=01fc3e3832e32ae8c12bf0c3b0819ca4a5972825
curl http://localhost:3000/news.json?key=01fc3e3832e32ae8c12bf0c3b0819ca4a5972825

# Username and password via HTTP Basic
curl "http://admin:test@localhost:3000/news.json"
curl "http://admin:test@localhost:3000/news.xml"

# Key via HTTP Basic
curl "http://01fc3e3832e32ae8c12bf0c3b0819ca4a5972825:@localhost/news.json"
curl "http://01fc3e3832e32ae8c12bf0c3b0819ca4a5972825:@localhost/news.xml"
curl "http://01fc3e3832e32ae8c12bf0c3b0819ca4a5972825:THE_PASSWORD_FIELD_CAN_BE_ANYTHING@localhost/news.json"
```

I also added the REST API to News (both XML and JSON). News was very simple and should be a good test of the system. The REST API can be enabled and disabled in the Redmine settings (disabled by default).

Committed in r3217, r3218, r3219, r3220

#9 - 2009-12-23 19:41 - Jean-Philippe Lang

I had to remove the mass creation of API keys for several reasons:

- not needed since keys will be created on the fly
- models should be used as less as possible in migrations
- took more than 10 minutes on my redmine database

Thanks for the feature.

#10 - 2009-12-24 18:43 - Eric Davis

Jean-Philippe Lang wrote:

> - took more than 10 minutes on my redmine database

Good point, thanks for the extra cleanup work on this. I'm going to try to write something small to demonstrate how to use it and see if there is anything else I missed.

#11 - 2010-06-01 12:22 - Vitaliy Ischenko

is there a rake task to manually generate api tokens?

#12 - 2010-10-20 23:09 - Ian Epperson

Eric Davis wrote:

> **This should be considered experimental until further testing.**
>
> I added a REST API for authentication with support for three styles of sending the credentials:
>
> - Key parameter - each user has an API token they can manage like the RSS tokens.
> - Username and password via HTTP Basic
> - Key via HTTP Basic

I started using this interface last night and it works rather well. There is a bug in that the key parameter will fail if asking for a single project or a single

issue:

```
GET http://my.server/projects/test.xml?key=1234..
GET http://my.server/issues/10.xml?key=1234..
```

The above works when using the Username/password via HTTP Basic, and asking for /projects.xml or /issues.xml works fine from either authentication.

#13 - 2010-10-20 23:23 - Ian Epperson

Just tried the key as the username and it works just fine.

#14 - 2010-10-21 02:41 - Eric Davis

Ian Epperson wrote:

> I started using this interface last night and it works rather well. There is a bug in that the key parameter will fail if asking for a single project or a single issue:

Yea, I've seen that. There are a few bugs in the projects and issues API when using the API keys. I'm going to do an audit of both apis for 1.1

#15 - 2010-10-21 09:47 - Ian Epperson

Awesome! Thanks Eric! I just published a Python library that uses the interface and have been trying to work around the holes. (My biggest wish at this point would be the ability to set assigned_to_name directly without trying to determine the user number.)

#16 - 2010-10-21 19:48 - Eric Davis

Ian Epperson wrote:

> Awesome! Thanks Eric! I just published a Python library that uses the interface and have been trying to work around the holes.

Great, I see you're added it to the wiki.

> (My biggest wish at this point would be the ability to set assigned_to_name directly without trying to determine the user number.)

Can you open a new issue for that? I think that would be a good option but this issue is closed so the discussion is done.

#17 - 2010-10-21 20:59 - Ian Epperson

Done. #6721

Got another one too: Allow some kind of set-user function to perform issue updates as if it were done by a different user without obtaining that user's password. I'll file it and note the use-case.

I can do this all day ;-)

#18 - 2018-03-21 12:37 - Dung Minh

It runs when i set: http://www.redmine.org/issues?key=AB458D45B2
Eric Davis wrote:

- API token via the url parameters - http://www.redmine.org/issues?api_key=AB458D45B2