Redmine - Feature #30086

Use HTTP status code 403 instead of 401 when REST API is disabled

2018-12-04 02:21 - Go MAEDA

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:	4.1.0		
Resolution:	Fixed		

Description

Currently, Redmine returns HTTP status code 401 (Unauthorized) if the REST API feature is disabled.

```
$ curl -D /dev/stdout --user admin:admin http://localhost:3000/issues.xml
HTTP/1.1 401 Unauthorized
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
Content-Type: application/xml
WWW-Authenticate: Basic realm="Redmine API"
Cache-Control: no-cache
X-Request-Id: 22e77bad-feca-4137-a81e-9df152af8bc2
X-Runtime: 0.019368
Transfer-Encoding: chunked
```

With the status code 401, users may misunderstand that the login id or password is incorrect. If they access to /issues.xml with a web browser, they will see a basic authentication dialog again and again.

I think it is proper and intuitive to return 403 (Forbidden) instead of 401, like "403 API access is not allowed".

Related issues:

Related to Redmine - Defect #32315: Impossible to validate API key without mo...	**Closed**

Associated revisions

Revision 18055 - 2019-04-10 04:51 - Go MAEDA

Use HTTP status code 403 instead of 401 when REST API is disabled (#30086).

Patch by Yuichi HARADA.

History

#1 - 2018-12-04 02:23 - Go MAEDA

- Description updated

#2 - 2018-12-10 03:20 - Yuichi HARADA

- File 30086-http-status-code-403.patch added

Regardless of whether authentication is valid or not, if you disable the REST API feature it responds with HTTP status code 403(Forbidden).
I made a patch, and attach it.

#3 - 2018-12-10 21:28 - Marius BĂLTEANU

I'm in favour of this change.

#4 - 2018-12-18 01:15 - Go MAEDA

- Target version set to 4.1.0

Setting the target version to 4.1.0.

#5 - 2019-01-18 01:56 - Go MAEDA

Returning 403 in the situation is consistent. In incoming emails API, MailHandlerController returns 403 if "WS for incoming emails" is disabled. Please see source:tags/4.0.0/app/controllers/mail_handler_controller.rb#L41.

#6 - 2019-02-25 13:34 - Go MAEDA

- File 30086-http-status-code-403-v2.patch added

Removed an unnecessary test_with_valid_username_and_wrong_password_http_authentication from the patch.

#7 - 2019-04-10 04:51 - Go MAEDA

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch. Thank you.

#8 - 2020-10-25 08:02 - Go MAEDA

- Related to Defect #32315: Impossible to validate API key without modifying anything added

Files

30086-http-status-code-403.patch	3.17 KB	2018-12-10	Yuichi HARADA
30086-http-status-code-403-v2.patch	2.7 KB	2019-02-25	Go MAEDA