Redmine - Defect #41220

API Access does not require second factor

2024-09-04 13:36 - Marco Descher

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	5.1.3

Description

I have configured a required second factor for the admin account.
This is enforced when logging in via the browser interface.

It is however **NOT** enforced when using the API, where using
https://my.redmine.org/my/account.json with basic authentication
delivers me my api key **NOT** requiring the second factor.

When getting a token for www.keycloak.org for example, it is required
to pass the HTTP header totp with the current value to the endpoint.

Related issues:

Related to Redmine - Feature #35001: Disable API authentication with username...	**Closed**

History

#1 - 2024-09-04 15:35 - Marco Descher

The same holds when accessing resources directly using their json or xml representation
e.g. https://my.redmine.org/issues.json

#2 - 2024-09-04 20:21 - Holger Just

- Status changed from New to Needs feedback

Redmine 5.1.3 does not allow to use basic authentication to access the API if two-factor authentication is enabled for a user. This was changed in #35001 starting with Redmine 5.0.0. My tests on a vanilla Redmine 5.0.3 confirms that this behavior works as intended, i.e. that API access is only possible with the user's API key if they have activated two-factor authentication but is denied when using the username and password with basic auth.

Accordingly, I'm unable to reproduce your described behavior. If you do still observe this however, please remove any plugins you may have installed and ensure that your Redmine code is unchanged. Please provide more details which allows us to reproduce this issue starting from a fresh Redmine.

#3 - 2024-09-04 20:21 - Holger Just

- Related to Feature #35001: Disable API authentication with username and password when two-factor authentication is enabled for the user added

#4 - 2024-09-04 20:35 - Marco Descher

Thank you for your feedback. I can confirm that my test by mistake went against a 4.2.8.stable instance, not the 5.1.3.
With 5.1.3 I can confirm, that the API returns HTTP 401. Thus this issue is resolved.

#5 - 2024-09-04 21:07 - Holger Just

- Status changed from Needs feedback to Closed

- Resolution set to Invalid

Thank you for your feedback.