Redmine - Feature #34070
Allow setting a grace period when forcing 2FA

2020-10-06 00:09 - Marius BALTEANU

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BALTEANU	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	Candidate for next major release		
Resolution:			

Description

On top of #31920 and #35439 which will allow to enable 2FA for certain groups or for administrators, we should add an option in admin to configure a grace period until the 2FA enforcement applies to all users.

In the grace period, the user should be redirected to the 2FA activation page after each successful login and informed about the enforcement, but with the option to skip the activation until enforcement date.

From my point of view, the simplest way is to add a new setting "Enforcement starting from" where the admin can choose the date.

Also, for new registered users, a similar grace period should be configurable, but in number of days.

Any feedback is welcome.

@Plan.io team, I have added you as watchers because the current implementation was provided by you and your feedback is important on all those issues related to 2FA.

Related issues:

Related to Redmine - Feature # 1237: Add support for two-factor authentication	**Closed**	**2008-05-14**
Related to Redmine - Feature # 35086: Please consider changing the way how 2F...	**Closed**	
Related to Redmine - Feature # 35439: Option to require 2FA only for users wi...	**Closed**	

History

#1 - 2021-04-19 09:13 - Marius BALTEANU

- Related to Feature #1237: Add support for two-factor authentication added

#2 - 2021-04-19 09:16 - Marius BALTEANU

- Related to Feature #35086: Please consider changing the way how 2FA is set up added

#3 - 2021-06-22 23:38 - Marius BALTEANU

- Description updated

#4 - 2022-01-23 22:27 - Marius BALTEANU

- Target version set to 5.0.0

#5 - 2022-01-24 11:11 - Marius BALTEANU

- File 0001-Allow-setting-a-grace-periond-before-requiring-two-f.patch added

- File user_flash.png added

- File grace_period_setting.png added

Here is a patch that adds a grace period setting (in hours) when an admin enables and requires two-factor authentication. This setting should simplify the activation process for instances with many users.

The grace period setting:
grace_period_setting.png

When the grace period is not expired, the user is redirected to twofa setup page and informed about the grace period, but he can skip the activation:
user_flash.png

Any feedback is welcome! The patch must be applied on top of #35439.

#6 - 2022-01-24 11:14 - Marius BALTEANU

- Related to Feature #35439: Option to require 2FA only for users with administration rights added

#7 - 2022-01-27 16:58 - Holger Just

I find the concept of an opaque timespan for a grace period rather unfortunate. For an admin, it is not clear when the grace period starts: When a user logs in next? When the setting is updated? Which setting? How can I know when it's updated?

On the settings screen it's also not clear when exactly the required status will finally be enforced.

As such, I'd rather propose to ask the admin to enter a fixed timestamp when the setting will be enforced. That would make things much clearer and also would allow to shorten or extend this as required.

For that, we would need:

- A UI for entering a date and time (not sure we have that somewhere yet?)
- Some server-side validation of the provided data format as we likely need to store an ISO8601 string in the DB

Apart from that, I think the 2FA activation check is only done on user login. A grace period of just a couple of hours thus might not result in a lot of users seeing the skip-option at all as existing sessions are not affected by the setting right now (correct me if I'm wrong here). A more common grace period would thus probably be a week or more.

Maybe it would also be helpful to forcefully kill existing sessions of users who have not enabled 2FA after the grace period has ended? Unfortunately, I'm not sure how we could do this in plain Redmine without either checking on every request or having a persisted job queue where we could schedule stuff in the future.

#8 - 2022-01-27 22:43 - Marius BALTEANU

Holger Just wrote:

> *I find the concept of an opaque timespan for a grace period rather unfortunate. For an admin, it is not clear when the grace period starts: When a user logs in next? When the setting is updated? Which setting? How can I know when it's updated?*
>
> *On the settings screen it's also not clear when exactly the required status will finally be enforced.*
>
> *As such, I'd rather propose to ask the admin to enter a fixed timestamp when the setting will be enforced. That would make things much clearer and also would allow to shorten or extend this as required.*

That was my initial solution, but I changed my mind thinking that this grace period can be used also for new users (in a future iteration). Also, I had in plan to display in the admin when the grace period expires, as I did for users in the enable 2FA page after login. Anyway, after your feedback, I think it's better to keep things simple and replace the grace period with a specific datetime.

> *For that, we would need:*
>
> - *A UI for entering a date and time (not sure we have that somewhere yet?)*
> - *Some server-side validation of the provided data format as we likely need to store an ISO8601 string in the DB*
>
> *Apart from that, I think the 2FA activation check is only done on user login. A grace period of just a couple of hours thus might not result in a lot of users seeing the skip-option at all as existing sessions are not affected by the setting right now (correct me if I'm wrong here). A more common grace period would thus probably be a week or more.*

You're right, existing sessions are not affected, the only differences compared with the "required" method are: - the redirect to enable 2FA page after user login

- the option to leave the page
- the notification regarding 2FA
- the grace period and when it ends.

> *Maybe it would also be helpful to forcefully kill existing sessions of users who have not enabled 2FA after the grace period has ended? Unfortunately, I'm not sure how we could do this in plain Redmine without either checking on every request or having a persisted job queue where we could schedule stuff in the future.*

Interesting option and it could be a good improvement from a security point of view because it covers also the cases with long session lifetime. Do you think it worths the effort?

Regarding the technical solution, I wouldn't check at any request, I prefer the queue option with a rake task that can be manually ran in case the queue is lost until the grace period ends (AsyncAdapter and a restart).

#9 - 2022-03-18 19:05 - Marius BALTEANU

- Target version changed from 5.0.0 to Candidate for next major release

Files

0001-Allow-setting-a-grace-periond-before-requiring-two-f.patch	11.2 KB	2022-01-24	Marius BALTEANU
grace_period_setting.png	85.7 KB	2022-01-24	Marius BALTEANU
user_flash.png	167 KB	2022-01-24	Marius BALTEANU