Redmine - Feature #35439

Option to require 2FA only for users with administration rights

2021-06-22 23:23 - Marius BĂLTEANU

Status:	Closed		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:	Marius BĂLTEANU		**% Done:**	0%
Category:	Accounts / authentication		**Estimated time:**	0.00 hour
Target version:	5.0.0			
Resolution:	Fixed			

Description

#31920 adds the option to enable 2FA only for certain groups when the 2FA setting is set to optional. This is very useful, but it doesn't cover the case when you want to enable 2FA only for administrators. As a best security practice, if you cannot enforce for all users, the administrators should be top priority to secure using 2FA.

My proposal is to add a new setting to allow enforcing 2FA only for administrators:

  2fa_optional.png
What do you think?

Related issues:

Related to Redmine - Feature #1237: Add support for two-factor authentication	**Closed**	**2008-05-14**
Related to Redmine - Feature #34070: Allow setting a grace period when forcin...	**New**	
Related to Redmine - Feature #31920: Require 2FA only for certain user groups	**Closed**	

Associated revisions

Revision 21395 - 2022-02-01 21:17 - Marius BĂLTEANU

Add "required for administrators" option to Two-factor authentication settings that behaves like optional, but will require all users with administration rights to set up two-factor authentication at their next login (#35439).

Revision 21396 - 2022-02-01 21:27 - Marius BĂLTEANU

Add locales (#35439).

History

#1 - 2021-06-22 23:24 - Marius BĂLTEANU

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

#2 - 2021-06-23 10:23 - Bernhard Rohloff

+1 I like the idea. It sounds very reasonable.
One thing I would like to mention is that it doesn't take much to remove the tick from the checkbox as an administrator without the other admins taking notice of the change.
Wouldn't it be better to have this setting in the configuration.yml to have more control on who can change it? Another option could be that every administrator gets notified if this option gets disabled.

#3 - 2021-06-23 10:34 - Marius BĂLTEANU

Bernhard Rohloff wrote:

> Wouldn't it be better to have this setting in the configuration.yml to have more control on who can change it? Another option could be that every administrator gets notified if this option gets disabled.

A notification sounds better to me.

#4 - 2021-11-14 06:43 - Alex JXXX

I think also it's the better way to add the option to force for admins.
If only one admin was set-up and he lost this phone. Any option exist to reset this OTP with SSH access ?

#5 - 2022-01-23 22:27 - Marius BĂLTEANU

- Target version set to 5.0.0

#6 - 2022-01-24 00:19 - Marius BĂLTEANU

- File 0001-Option-to-require-2FA-authentication-only-for-users-.patch added

Here is a patch that I would like to commit in the following days.

#7 - 2022-01-24 11:14 - Marius BĂLTEANU

- Related to Feature #34070: Allow setting a grace period when forcing 2FA added

#8 - 2022-01-27 13:52 - Holger Just

- Related to Feature #31920: Require 2FA only for certain user groups added

#9 - 2022-01-27 14:05 - Holger Just

I think this general idea of enforcing 2FA for admins only, might a good idea to allow people to simplify this transition.

Right now, a workaround for that would be to create a group with all admin users and force 2fa for this group. With this setting, people would be relieved from having to maintain a separate group for that while still protecting the most important users.

However, I'm thinking whether it wouldn't be more sensible to introduce an additional possible value for Setting.twofa instead of this separate setting (and thus just an additional option in the dropdown)? This could look like this (as a rough sketch):

```
class Setting
  #...
  def self.twofa_required?
    twofa == '2'
  end

  def self.twofa_optional?
    %w[1 3].include? twofa
  end

  def self.twofa_required_for_administrators?
    twofa == '3'
  end
end

class User
  # ...

  def must_activate_twofa?
    return false if twofa_active?

    return true if Setting.twofa_required?
    return true if Setting.twofa_required_for_administrators? && admin?
    return true if Setting.twofa_optional? && groups.any?(&:twofa_required?)

    false
  end
end
```

What do you think?

#10 - 2022-01-27 21:07 - Marius BĂLTEANU

Thank you, Holger!

Holger Just wrote:

> I think this general idea of enforcing 2FA for admins only, might a good idea to allow people to simplify this transition.
>
> Right now, a workaround for that would be to create a group with all admin users and force 2fa for this group. With this setting, people would be relieved from having to maintain a separate group for that while still protecting the most important users.

I totally agree with you, this is way I created this ticket.

> However, I'm thinking whether it wouldn't be more sensible to introduce an additional possible value for Setting.twofa instead of this separate setting (and thus just an additional option in the dropdown)? This could look like this (as a rough sketch):
>
> [...]

What do you think?

Great ideea, thank you! I'm going to update the patch.

#11 - 2022-01-27 22:15 - Marius BĂLTEANU

- File 0001-Option-to-require-2FA-authentication-only-for-users-.patch added

Here is the updated version, all [tests pass](). Thanks again Holger for your feedback!

On a related topic, do you know why was added a new local ([label_required_lower]()) instead of using downcase on the existing one ([label_required]())?

#12 - 2022-01-28 12:21 - Holger Just

Thank you Marius for taking care of this!

I think the new option should work kind of like "optional, but required for admins". The possibility of to also enforce 2FA for members of specific groups should still be possible with this setting.

Because of that, I proposed to return true in Setting.twofa_optional? above. If you don't want to do that, at least the view in app/views/groups/_form.html.erb would have to be adapted for the new option (or it may have to in any case, I not entirely sure now)

As for User#must_activate_twofa?, I personally like my proposed option better stylisticly because I think the rules are much easier to understand rather than having to parse nested boolean algebra. The result should be exactly the same. The original method was borderline okay with just a few rules. But now with the additional ones, I think we should refactor the method.

#13 - 2022-01-29 17:59 - Felix Schäfer

Marius BALTEANU wrote:

> On a related topic, do you know why was added a new local ([label_required_lower]()) instead of using downcase on the existing one ([label_required]())?

downcase might work somewhat OK for languages with latin scripts (and even then, in German nouns start with a capital no matter where they are in a sentence, which would not be a problem in this case but might be in others), but that's not something that will work reliably for arbitrary locales.

I agree that the choice of the name for the locale key is a little unfortunate, but it was chosen to resemble the _plural keys for example.

#14 - 2022-01-30 11:17 - Marius BĂLTEANU

- File 0001-Option-to-require-2FA-authentication-only-for-users-.patch added

- File hints.png added

- File options.png added

Holger Just wrote:

> Thank you Marius for taking care of this!
>
> I think the new option should work kind of like "optional, but required for admins". The possibility of to also enforce 2FA for members of specific groups should still be possible with this setting.

I totally miss that from the updated version of the patch, thanks for pointing this out.

> Because of that, I proposed to return true in Setting.twofa_optional? above. If you don't want to do that, at least the view in app/views/groups/_form.html.erb would have to be adapted for the new option (or it may have to in any case, I not entirely sure now)

First option sounds good to me as well.

> As for User#must_activate_twofa?, I personally like my proposed option better stylisticly because I think the rules are much easier to understand rather than having to parse nested boolean algebra. The result should be exactly the same. The original method was borderline okay with just a few rules. But now with the additional ones, I think we should refactor the method.

I've already committed this change as part of [#31920]().

I'm attaching a new version which should work as expected. The patch adds the option "required for administrators" in the Two-factor authentication dropdown, between optional and required with the following hint: "Setting required for administrators behaves like optional, but will require all users with administration rights to set up two-factor authentication at their next login."

Some screenshots:
   options.png

   hints.png
Are the translations clear enough? Or is it better "optional, but required for administrators"?

#15 - 2022-01-30 11:18 - Marius BĂLTEANU

Felix Schäfer wrote:

> Marius BALTEANU wrote:
>
> > On a related topic, do you know why was added a new local ([label_required_lower](#)) instead of using downcase on the existing one ([label_required](#))?
>
> downcase might work somewhat OK for languages with latin scripts (and even then, in German nouns start with a capital no matter where they are in a sentence, which would not be a problem in this case but might be in others), but that's not something that will work reliably for arbitrary locales.
>
> I agree that the choice of the name for the locale key is a little unfortunate, but it was chosen to resemble the _plural keys for example.

Thanks Felix for your response, it's clear now.

#16 - 2022-01-30 14:18 - Holger Just

Thank you for taking care of the changes!

Marius BALTEANU wrote:

> Are the translations clear enough? Or is it better "optional, but required for administrators"?

I think the option name is clear along with the explanatory text below.

#17 - 2022-02-01 21:18 - Marius BĂLTEANU

- Status changed from New to Closed

- Resolution set to Fixed

Feature added in [r21395](#).

#18 - 2022-02-01 21:19 - Marius BĂLTEANU

- Status changed from Closed to Reopened

#19 - 2022-02-01 21:19 - Marius BĂLTEANU

- Status changed from Reopened to Resolved

#20 - 2022-02-01 23:21 - Marius BĂLTEANU

- Status changed from Resolved to Closed

Files

2fa_optional.png	83.9 KB	2021-06-22	Marius BĂLTEANU
0001-Option-to-require-2FA-authentication-only-for-users-.patch	4.24 KB	2022-01-23	Marius BĂLTEANU
0001-Option-to-require-2FA-authentication-only-for-users-.patch	5.3 KB	2022-01-27	Marius BĂLTEANU
0001-Option-to-require-2FA-authentication-only-for-users-.patch	4.93 KB	2022-01-30	Marius BĂLTEANU
options.png	88 KB	2022-01-30	Marius BĂLTEANU
hints.png	79.7 KB	2022-01-30	Marius BĂLTEANU