redmineorg-copy202205 - Vote #64996

Lock accounts after X failed attempts

2022/05/09 13:58 - Admin Redmine

ステータス:	New	**開始日:**	2009/04/01
優先度:	高め	**期日:**	
担当者:		**進捗率:**	50%
カテゴリ:	Accounts / authentication_7	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/3096	**status_id:**	1
category_id:	7	**tracker_id:**	2
version_id:	0	**plus1:**	4
issue_org_id:	3096	**affected_version:**	
author_id:	4827	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	17		

説明

I believe Redmine should have the functionality available to put accounts in to a locked state after so many failed login attempts. The number of failed attempts should be configurable via the Administration panel. Notification to an administrator e-mail address that the account was locked is desired as well.

I am surprised this feature has not made it in to Redmine yet. Could this be something that makes it in to a 0.9 release? I plan on exposing my Redmine instance to more than just internal folk within the next 6mo-1yr. I do not want to give any external entity the ability to brute force my password.

journals

+1

+ function to email admin/user about locking. Also account can be optionally unlocked after some (probably configurable) period, like 1 hour...

+1 (failed attempts number should be configurable)

Automatic unlocking after some period might be security problem.

+1
I also think this might be very useful.

I just started working on a patch for this.

I am almost done with the patch but was wondering how accounts should be unlocked.
I can see the following alternatives:

After a timeout, as suggested earlier

Notification email contains a link that will unlock the account again

You have to deal with an admin outside the system and he has to manually unlock it

Go through "forgot password" and reset the password and when the password is reset the account will be unlocked.

I personally think that 2. would be best.

Any thoughts about this or other suggestions?

#4 isn't a viable option since my LDAP is read-only and I don't even know if "Forgot password" works with LDAP (probably not).

It would be best if the admin is given the option to configure #1, #2, or #3, but I'll take either #2 or #3.

I implemented solution 2. Although if there is need it should be very easy to add an option to use 3. in addition.

Attached is a patch that should allow the admin to define a number of allowed login attempts and the address of an admin.
If a user fails to login the flash-message will show how many logins are left. If none are left the flash tells so and the account gets locked. A mail informing the provided admin address will be send. The suer will also receive a mail telling him what happened and providing a link to reactivate the account.

However since I am a bad boy I didn't write unit tests yet. So there still might be something wrong. I will provide another patch which will include tests later this week.

Thanks Alexander. Once you add some unit tests I'll be able to take a closer look at applying this patch. From a quick glance @User#authentication_failed@ could be cleaned up a bit. I see two calls to @self.save!@ and no handling of their failure cases.

I added a unit test and changed the two 'save!'s to 'save' since I could not come up with a useful way to catch a failed save.

Please let me know if and how I can improve the patch further!

Great, I really need this.

I'm curious if anybody has been running this patch in their environment... What are your thoughts? Anything that could be improved?

Is this still the only method to lock accounts after failed retries ? Does it work with the current version of redmine ?

I believe this feature would improve a lot redmine security. Giving more confidence to me and my clients.

---

duplicate of #3155

@ go2null wrote:

> duplicate of #3155

Not completely. #3155 is older than this issue and it is much more generic, while this issue is specific to one requested change. So I'll add a relation, but won't close this one as duplicate.

+1

related_issues

relates,New,3155,Password policy and secure logon procedure

履歴

#1 - 2022/05/10 17:26 - Admin Redmine

- カテゴリ を Accounts / authentication_7 にセット