

Redmine - Feature #33216

/my/account: Prevent users from changing their Email [redmine 4.1.0 stable]

2020-03-30 10:26 - James Barrante

Status:	New	Start date:									
Priority:	Normal	Due date:									
Assignee:		% Done:	0%								
Category:	Accounts / authentication	Estimated time:	0.00 hour								
Target version:											
Resolution:											
Description											
<p>An organization's policy requires users not be able to change their Redmine e-mail address.</p> <p>(Extra background/scenario info: User registration, Project and Role assignment is done by a script which also uses the autologin cookie feature of Redmine: User clicks a link from an Intranet page, that script handles above user creation tasks (if user doesn't exist yet) and logs him/her into Redmine, without ever requiring them to enter a password for Redmine. Logout is done by having Apache redirect the "/logout" script to some different URL on the Intranet which also clears the Redmine session cookies.) So far, we are very happy and thankful to all Redmine Contributors.</p> <p>While it is possible to change the number of extra e-mail addresses from 5 (default) to 0 [Administration > Settings > Users > Maximum number of additional email addresses], it still means that (under /my/account) any user logged in is able to change their e-mail address, unless the e-mail address is already taken by someone else in the system.</p> <p>Having an Administration setting to "lock" only the Email address of an account would be great. It could help enforce policy of only using the organization's e-mail addresses.</p> <p>From debug production.log, when a user updates his Email:</p> <pre>EmailAddress Update (0.2ms) UPDATE `email_addresses` SET `address` = '[redacted]', `updated_on` = '2020-03-29 18:55:59' WHERE `email_addresses`.`id` = 2</pre> <p>Hacking I tried:</p> <ul style="list-style-type: none">• As a Ruby novice, I really am having a rough time finding my way through the code. Thanks to MVC, I don't believe it's as easy as just commenting out a line of code responsible for triggering the above SQL? Any pointer would be greatly appreciated.• Maybe app/controllers/email_addresses_controller.rb would be a place to start, but I'm not sure. <p>Feature request:</p> <ul style="list-style-type: none">• Add a Checkbox under Administration > Settings > Users: Allow users to change their email addresses, checked by default <p>"Workarounds":</p> <ul style="list-style-type: none">• Apache Rewrite Rule to block access to /my/account altogether. Easy to implement, radical and effective, but not very friendly, as some useful Preferences (Time zone, UI Language) will be unavailable to users.• Cronjob to replay any changed e-mail addresses to the MySQL database. Doesn't feel right.• MySQL trigger to roll back any UPDATE statement to the `email_addresses` table. Hackish but better than cron; will likely break once a heavier DB Migrate script runs after updating Redmine. <tr><td colspan="4">Related issues:</td></tr> <tr><td colspan="2">Related to Redmine - Feature #3369: Allowed/Disallowed email domains settings...</td><td>Closed</td><td>2009-05-16</td></tr>				Related issues:				Related to Redmine - Feature #3369: Allowed/Disallowed email domains settings...		Closed	2009-05-16
Related issues:											
Related to Redmine - Feature #3369: Allowed/Disallowed email domains settings...		Closed	2009-05-16								

History

#1 - 2020-03-31 09:07 - Go MAEDA

- Related to Feature #3369: Allowed/Disallowed email domains settings to restrict users' email addresses added

#2 - 2020-03-31 09:18 - Go MAEDA

James Barrante wrote:

Having an Administration setting to "lock" only the Email address of an account would be great. It could help enforce policy of only using the organization's e-mail addresses.

In [#3369](#), a feature is proposed that would allow users to only use email addresses from domains that are pre-allowed.

The feature is different from the one proposed here, but I think your request "enforce policy of only using the organization's e-mail addresses" can be achieved.

Would it be helpful to you if [#3369](#) was implemented?

#3 - 2020-03-31 10:11 - James Barrante

Thank you, Go MAEDA.

Would it be helpful to you if [#3369](#) was implemented?

In certain ways, yes. It could help in a scenario where only one organization (or a small set thereof) is served. It would not prevent address changes in the form of <[User11@A-Corp.com](#)> to <[User22@Z-Corp.com](#)>, if both domains are in the whitelist. But it could certainly improve things for the outlined scenario.

However, please still consider a lockdown on the email address.