To improve the security of a fresh Redmine installation, I propose to force a password reset for the default admin account on first login.

If this change is applied, the installation instructions would need to be updated accordingly.

Unit test should not be affected, since they solely rely on fixtures and not default data created using migrations.

The attached patch, adds a migration which sets the `must_change_passwd` field to `true` for the default admin account, if it was not used yet (`last_login_on: nil`). This should make sure, that existing installations are not affected and the changes are only applied during the initial `rake db:migrate` run.

**Related issues:**
- Related to Redmine - Patch # 3858: Force the 'admin' account to change the default password

**Associated revisions**

**Revision 15321 - 2016-04-11 21:07 - Jean-Philippe Lang**

Force password reset for default admin user (#22381).

Patch by Gregor Schmidt.

**History**

**#1 - 2016-04-04 11:31 - Go MAEDA**
- Related to Patch #3858: Force the 'admin' account to change the default password added

**#2 - 2016-04-11 12:53 - Gregor Schmidt**

Thanks for pointing me to the other ticket. Before creating this issue, I was trying to find a similar ticket, but I guess, I was using the wrong search terms.

I just had a look at the patch, you proposed in #3858. It looks, like we both had the same idea. :) Therefore I would propose to close this issue in favour of #3858. (Unfortunately I cannot do that on my own.)

I just wanted to briefly explain, that I was hesitant to create a User instance within the migration, since that sometimes leads to errors involving outdated column caches within ActiveRecord.

**#3 - 2016-04-11 21:09 - Jean-Philippe Lang**
- Status changed from New to Closed
- Assignee set to Jean-Philippe Lang
Gregor Schmidt wrote:

I just wanted to briefly explain, that I was hesitant to create a User instance within the migration, since that sometimes leads to errors involving outdated column caches within ActiveRecord.

Agreed, using model instances in migrations should be avoided as much as possible. Patch committed.

#### #4 - 2016-05-21 09:12 - Jean-Philippe Lang
- Subject changed from Require password reset on initial setup to Require password reset on initial setup for default admin account

**Files**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-Force-password-reset-for-default-admin-user.patch</td>
<td>1020 Bytes</td>
<td>2016-04-04</td>
<td>Gregor Schmidt</td>
</tr>
</tbody>
</table>