

## Foreman - Feature #5585

### Support non-md5 root password

05/06/2014 01:22 PM - Vincent Brillault

|  |                                 |
|--|---------------------------------|
| <b>Status:</b> Duplicate   |                                 |
| <b>Priority:</b> Normal  |                                 |
| <b>Assignee:</b>   |                                 |
| <b>Category:</b>   |                                 |
| <b>Target version:</b>   |                                 |
| <b>Difficulty:</b>   | <b>Fixed in Releases:</b>       |
| <b>Triaged:</b>  | <b>Found in Releases:</b>       |
| <b>Bugzilla link:</b>  | <b>Red Hat JIRA:</b>            |
| <b>Pull request:</b>   |                                 |
| <b>Description</b>   |                                 |
| <p>When adding a root password in a hostgroup, Foreman automatically add a salt and hashes it using the md5 algorithm.</p> <p>Could it be possible to support other, more recent, algorithms, for example SHA-256 or SHA-512 and even blowfish where it is implemented?</p> <p>I do not know the code, but a simple grep seems to indicate that the following code is responsible for this:<br/>(<a href="https://github.com/theforeman/foreman/blob/develop/app/models/concerns/host_common.rb#L108">https://github.com/theforeman/foreman/blob/develop/app/models/concerns/host_common.rb#L108</a>)<br/>self.root_pass = root_pass.empty? ? nil : (root_pass.starts_with?('\$') ? root_pass :<br/>root_pass.crypt("\$1\${SecureRandom.base64(6)}"))</p> <p>The '1' in the "\$1\$" here is problematic.<br/>Could it be changed to a configuration option (with '1' used by default) ?</p> <p>Thanks in advance,<br/>Vincent</p> <p>PS: during my greping, I found another part using the root password:<br/>(<a href="https://github.com/theforeman/foreman/blob/develop/app/helpers/unattended_helper.rb#L9">https://github.com/theforeman/foreman/blob/develop/app/helpers/unattended_helper.rb#L9</a>)<br/>def grub_pass<br/>@grub ? "--md5pass=#{@host.root_pass}": ""<br/>end<br/>This is likely to break if root_pass is not a md5 password.</p> |                                 |
| <b>Related issues:</b>   |                                 |
| Is duplicate of Foreman - Feature #2127: Support newer hash schemes for root ...   | <b>Closed</b> <b>01/15/2013</b> |

#### History

##### #1 - 05/06/2014 01:26 PM - Dominic Cleal

- Is duplicate of Feature #2127: Support newer hash schemes for root passwords added

##### #2 - 05/06/2014 01:27 PM - Dominic Cleal

- Status changed from New to Duplicate

Thanks for the report, we're tracking this under [#2127](#) (it's high up on our backlog too I think).

##### #3 - 05/06/2014 01:40 PM - Vincent Brillault

Sorry, I missed this one (I searched for root password, but did not find it).  
Thanks.

##### #4 - 09/04/2014 03:39 PM - The Foreman Bot

- Target version set to 1.7.4

- Pull request <https://github.com/theforeman/foreman/pull/1736> added

**#5 - 09/05/2014 04:25 AM - Dominic Cleal**

- *Target version deleted (1.7.4)*
- *Pull request added*
- *Pull request deleted (<https://github.com/foreman/foreman/pull/1736>)*