

Redmine - Defect #34234

Use Setting.host_name instead of Setting.app_title as TOTP issuer to avoid name collision with other instances or apps

2020-11-08 14:13 - Go MAEDA

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Go MAEDA	% Done:	0%
Category:	Accounts / authentication	Estimated time:	0.00 hour
Target version:		Affected version:	
Resolution:	Fixed		
Description			
<p>Currently, Redmine's two-factor authentication uses Setting.app_title for TOTP issuer. However, it causes problems under certain conditions.</p> <p>Suppose that you use Microsoft Authenticator and have access to the following two Redmine instances:</p> <ul style="list-style-type: none">- Redmine-1: host_name = "redmine.example.com", app_title = "Redmine", login = "jsmith"- Redmine-2: host_name = "redmine.example.org", app_title = "Redmine", login = "jsmith" <p>Enabling two-factor authentication for Redmine-1 is no problem.</p> <p>However, a serious problem occurs when you have enabled two-factor authentication for the Redmine-2. Surprisingly, Microsoft Authenticator overwrites the existing account information for Redmine-1 in order to add the account information for Redmine-2. This is because the exactly same TOTP issuer ("Redmine") and account ("jsmith") is used in two Redmine instances. These two values may play a role in the primary key in Microsoft Authenticator.</p> <p>I don't think the possibility of such an accident occurs is low in the real world because there are many instances that uses default app_title "Redmine". Or if the Redmine's app_title is set to "GitHub", GitHub's account in the Microsoft Authenticator will be overwritten with Redmine's account!</p> <p>In order to reduce the probability of such accidents, I suggest using Setting.host_name instead of Setting.app_title for TOTP issuer string. Most admins set the appropriate value for Setting.host_name to make links in email notifications correct. And this value does not usually overlap with other Redmine instances. GitLab also uses host name for TOTP issuer string.</p> <pre>diff --git a/lib/redmine/twofa/totp.rb b/lib/redmine/twofa/totp.rb index e304208a2..b714c78c7 100644 --- a/lib/redmine/twofa/totp.rb +++ b/lib/redmine/twofa/totp.rb @@ -63,7 +63,7 @@ module Redmine private def totp - @totp = ROTP::TOTP.new(@user.twofa_totp_key, issuer: Setting.app_title) + @totp = ROTP::TOTP.new(@user.twofa_totp_key, issuer: Setting.host_name) end end end</pre>			
Related issues:			
Related to Redmine - Feature # 1237: Add support for two-factor authentication		Closed	2008-05-14

Associated revisions

Revision 20308 - 2020-11-09 07:37 - Go MAEDA

Use Setting.host_name instead of Setting.app_title as TOTP issuer to avoid name collision with other instances or apps (#1237, #34234).

History

#1 - 2020-11-08 14:14 - Go MAEDA

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

#2 - 2020-11-09 01:03 - Mizuki ISHIKAWA

This specification looks good.

Since app_title often uses company name and project name, there is a risk of overwriting and deleting the account information of services other than Redmine that use those names.

I think the issuer should use a complex name that is hard to duplicate, such as a host name.

#3 - 2020-11-09 03:55 - Go MAEDA

- *Subject changed from Use Setting.host_name instead of Setting.app_title for TOTP issuer to Use Setting.host_name instead of Setting.app_title as TOTP issuer to avoid name collision with other instances or apps*

#4 - 2020-11-09 07:38 - Go MAEDA

- *Status changed from New to Closed*
- *Assignee set to Go MAEDA*
- *Resolution set to Fixed*

Committed the fix as a part of #1237.