redmineorg-copy202205 - Vote #78102

Force SSL when Setting.protocol is "https"

2022/05/09 18:10 - Admin Redmine

ステータス:	New	**開始日:**	2022/05/09
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Administration_8	**予定工数:**	0.00時間
対象バージョン:	Candidate for next major release_32	**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/24763	**status_id:**	1
category_id:	8	**tracker_id:**	2
version_id:	32	**plus1:**	1
issue_org_id:	24763	**affected_version:**	
author_id:	5107	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	14		

説明

Forcing SSL is important, and some enterprise environment can't be used if they aren't forcing the SSL due to security standards and best practices.

Redmine's *Administration ¦ Settings* offers *HTTPS* as an option, but choosing it +does nothing+.
!redminessl.png!

Editing the config/settings.yml and changing protocol from default: http
to https does nothing also

However placing the

@config.force_ssl = true@

in config/application.rb do work and do force SSL

So I'm not sure is it a defect or a feature request, but I'm posting it as a defect.

My Redmine info:

Environment:
Redmine version 3.3.1.stable
Ruby version 2.1.4-p265 (2014-10-27) [x86_64-linux]
Rails version 4.2.7.1
Environment production
Database adapter Mysql2

journals

Aleksandar Pavic wrote:

> Redmine's *Administration ¦ Settings* offers *HTTPS* as an option, but choosing it +does nothing+.

It is used to generate URL of issues in email notification.

+1

Confirmed in 3.4.6

placing config.force_ssl = true anywhere in config/application.rb

makes it work the rails way...

As I have explained back in 2017 [[[http://www.redminecookbook.com/blog-29-Forcing-Redmine-to-use-SSL-on-Apache]]]

I can confirm this issues still prevails on

```
Redmine version 4.1.0.stable.19444
Ruby version 2.6.5-p114 (2019-10-01) [x86_64-linux]
Rails version 5.2.4.1
```

fixing with force_ssl = true works.

I agree that Redmine default settings should contain better security settings. For now, I propose to enforce SSL on production environment. "Let's Encrypt":https://letsencrypt.org/ it's a good option for those who don't want to buy a certificate.

```
diff --git a/config/environments/production.rb b/config/environments/production.rb
index 16d9fc2f7..99632ca26 100644
--- a/config/environments/production.rb
+++ b/config/environments/production.rb
@@ -24,4 +24,7 @@ Rails.application.configure do

   # Print deprecation notices to the Rails logger.
   config.active_support.deprecation = :log
+
+  # Enforce secure HTTP requests
+  config.force_ssl = true
 end
```

@Marius

that code enforces SSL always, what I'm alluding is that if you choose in settings to use HTTPS,
then force_ssl = true should be set...

Unfortunately I can't write code and test, at the moment...

Marius BALTEANU wrote:

> I agree that Redmine default settings should contain better security settings. For now, I propose to enforce SSL on production environment. "Let's Encrypt":https://letsencrypt.org/ it's a good option for those who don't want to buy a certificate.

I think it is overkill. There are many cases running Redmine in production mode as follows:

- Using Redmine on intranet with an internal hostname such as http://192.168.1.1/ or http://redmine.test/
- An environment that Redmine has been just installed and application for a certificate has not been completed
- Developers who test Redmine in both development and production mode

Enforcing SSL for production mode complicates the installation process for those usecases may make admins spent a lot of time to troubleshoot.

My original post, is that changing from http to https in settings, does nothing, you don't get redirected to https...

We can either remove that setting, since it doesn't do anything...

Or make it work, by having it set force_ssl = true, since only then users get redirected to https...

Maybe there is some other way to make it work that I'm unaware of.

Go MAEDA wrote:

> Marius BALTEANU wrote:
>
> > I agree that Redmine default settings should contain better security settings. For now, I propose to enforce SSL on production environment. "Let's Encrypt":https://letsencrypt.org/ it's a good option for those who don't want to buy a certificate.
>
> I think it is overkill. There are many cases running Redmine in production mode as follows:
>
> - Using Redmine on intranet with an internal hostname such as http://192.168.1.1/ or http://redmine.test/
> - An environment that Redmine has been just installed and application for a certificate has not been completed
> - Developers who test Redmine in both development and production mode
>
> Enforcing SSL for production mode complicates the installation process for those usecases may make admins spent a lot of time to troubleshoot.

These are valid points, even if these type of tests should not be made on "production" mode and even in intranet they should use https. Some companies are using self signed certificates which are trusted in their internal network. I'll think to a better solution.

Aleksandar Pavic wrote:

> My original post, is that changing from http to https in settings, does nothing, you don't get redirected to https...
>
> We can either remove that setting, since it doesn't do anything...
>
> Or make it work, by having it set force_ssl = true, since only then users get redirected to https...
>
> Maybe there is some other way to make it work that I'm unaware of.

It does, please see #24763#note-1.

I think the decision to use SSL or not should be made by a server admin. And enforcing SSL in the next version is a too drastic change.

I suggest modifying the patch in #24763#note-8 as follows.

```
diff --git a/config/environments/production.rb b/config/environments/production.rb
index 16d9fc2f7..3e16e42ad 100644
--- a/config/environments/production.rb
+++ b/config/environments/production.rb
@@ -24,4 +24,8 @@ Rails.application.configure do
 
   # Print deprecation notices to the Rails logger.
   config.active_support.deprecation = :log
+
+  # Enforce secure HTTP requests
+  # Uncommenting the following line is HIGHLY RECOMMENDED
+  # config.force_ssl = true
 end
```

I want a lot of people to try Redmine casually. So, I am opposed to complicating the installation process by forcing an ideal and perfect configuration.

Ok, so may I suggest adding a feature then, because most people aren't messing with anything except config.yml and database.yml

!redmine_https.png!

or

!https_always.png!

if

@config.force_ssl = true@

can be set programatically during runtime...

related_issues

relates,New,2579,Configure SSL schema for "private" actions.
relates,New,3804,Authentication over HTTPS

履歴

#1 - 2022/05/10 17:06 - Admin Redmine

- カテゴリ を Administration_8 にセット

- 対象バージョン を Candidate for next major release_32 にセット