

## Redmine - Defect #35226

### Add SameSite=Lax to cookies to fix warnings in web browsers

2021-05-11 10:11 - Go MAEDA

<b>Status:</b>	Closed	<b>Start date:</b>	
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Go MAEDA	<b>% Done:</b>	0%
<b>Category:</b>	Accounts / authentication	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	4.1.4	<b>Affected version:</b>	
<b>Resolution:</b>	Fixed		

#### Description


Firefox 88.0.1 shows the following warning in Web Console.

Cookie “\_redmine\_session” will be soon rejected because it has the “SameSite” attribute set to “None” or an invalid value, without the “secure” attribute. To know more about the “SameSite” attribute, read <https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite>

According to [https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#fixing\\_common\\_warnings](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#fixing_common_warnings), we have two options to fix the warning:

1. Add Secure attribute to the cookie
2. Set SameSite attribute to the value other than "None"

However, if you set the Secure attribute, Redmine cannot be used in non-HTTPS environments such as test environments and some on-premise servers. Therefore, I think it is preferable to set the SameSite attribute to something other than "None".



#### Associated revisions

##### Revision 21009 - 2021-05-27 10:31 - Go MAEDA

Add SameSite=Lax to cookies to fix warnings in web browsers (#35226).

Patch by Go MAEDA.

##### Revision 21037 - 2021-06-16 16:15 - Go MAEDA

Merged r21009 from trunk to 4.2-stable (#35226).

##### Revision 21038 - 2021-06-16 16:17 - Go MAEDA

Merged r21009 from trunk to 4.1-stable (#35226).

#### History

##### #1 - 2021-05-11 10:35 - Go MAEDA

The following patch fixes the issue.

The patch must be safe because Redmine's cookie is already treated as SameSite=Lax in Chrome.

Redmine does not explicitly set the SameSite attribute in the Set-Cookie field. So, it is treated as SameSite=Lax in Chrome 80 and later.  
<https://blog.chromium.org/2020/02/samesite-cookie-changes-in-february.html>

```
diff --git a/config/application.rb b/config/application.rb
```

```

index dc8d5f89d..fc6e6a33f 100644
--- a/config/application.rb
+++ b/config/application.rb
@@ -79,7 +79,8 @@ module RedmineApp
  config.session_store(
    :cookie_store,
    :key => '_redmine_session',
-    :path => config.relative_url_root || '/'
+    :path => config.relative_url_root || '/',
+    :same_site => :lax
  )

  if File.exists?(File.join(File.dirname(__FILE__), 'additional_environment.rb'))

```

## #2 - 2021-05-11 11:19 - Liane Hampe

I can confirm that it is working in Firefox 88.0.1 when running Redmine 4.2 in production!

## #3 - 2021-05-12 04:12 - Go MAEDA

- Subject changed from *Warning about cookies with SameSite=none to Warning due to cookies not having SameSite attribute set*
- Category set to *Accounts / authentication*
- Target version set to *4.1.4*

Setting the target version to 4.1.4.

## #4 - 2021-05-13 08:35 - Go MAEDA

- File *35226-v2.patch* added

Updated the patch. Another two cookies "autologin" and "history\_last\_tab" also needs to have "SameSite=Lax".

## #5 - 2021-05-27 10:31 - Go MAEDA

- Subject changed from *Warning due to cookies not having SameSite attribute set to Add SameSite=Lax to cookies to fix warnings in web browsers*
- Status changed from *New to Resolved*
- Assignee set to *Go MAEDA*
- Resolution set to *Fixed*

Committed the patch.

## #6 - 2021-06-16 16:17 - Go MAEDA

- Status changed from *Resolved to Closed*

## Files

samesite-none-warning.png	108 KB	2021-05-11	Go MAEDA
35226-v2.patch	1.5 KB	2021-05-13	Go MAEDA