单点登录集成，通过谷歌浏览器80版本及以上访问Smartbi报表，有时会跳转到Smartbi登录界面

（本文档仅供参考）

问题现象

1、2020年3月份有用户反馈，在第三方系统通过iframe的方式集成Smartbi的url，并拼接了登录信息从而实现单点登录，在谷歌浏览器（80版本）中，打开报表有时会跳到Smartbi登录界面（现象如下图所示），通过IE、火狐等其他浏览器访问是正常的。

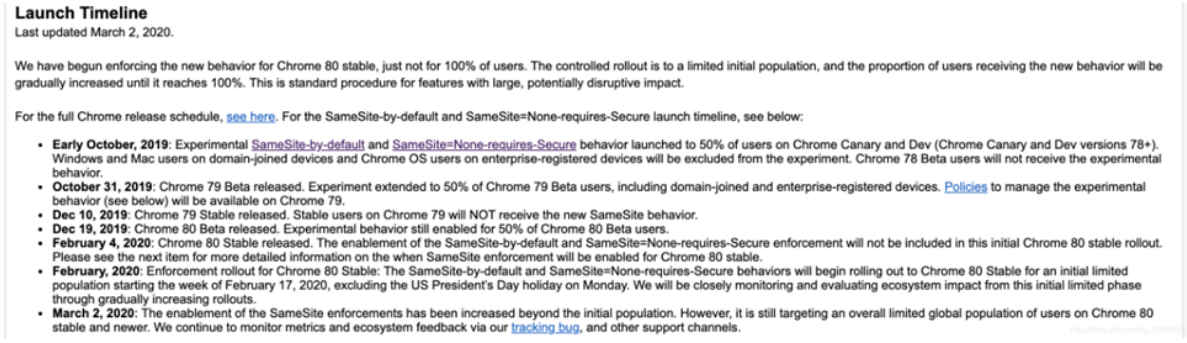
2、基于 Chromium 开源项目的内核浏览器，如新版本的Microsoft Edge浏览器，第三方系统拼接了登录信息集成smartbi，也会存在跳到Smartbi登录界面的问题。

问题分析

1. 问题的本质

新版本的chrome浏览器（80版本之后）对cookie的校验更加严格，SameSite属性默认值由None变为Lax，在SameSite属性为Lax的情况下，跨域是不允许传递cookie的，未传递cookie则单点登录失败。

详情请见：　　https://blog.csdn.net/qq_37788558/article/details/104484888?fps=1&locationNum=2



Launch Timeline

Last updated March 2, 2020.

We have begun enforcing the new behavior for Chrome 80 stable, just not for 100% of users. The controlled rollout is to a limited initial population, and the proportion of users receiving the new behavior will be gradually increased until it reaches 100%. This is standard procedure for features with large, potentially disruptive impact.

For the full Chrome release schedule, see here. For the SameSite-by-default and SameSite=None-requires-Secure launch timeline, see below:

- **Early October, 2019**: Experimental SameSite-by-default and SameSite=None-requires-Secure behavior launched to 50% of users on Chrome Canary and Dev (Chrome Canary and Dev versions 78+). Windows and Mac users on domain-joined devices and Chrome OS users on enterprise-registered devices will be excluded from the experiment. Chrome 78 Beta users will not receive the experimental behavior.
- **October 31, 2019**: Chrome 79 Beta released. Experiment extended to 50% of Chrome 79 Beta users, including domain-joined and enterprise-registered devices. Policies to manage the experimental behavior (see below) will be available on Chrome 79.
- **Dec 10, 2019**: Chrome 79 Stable released. Stable users on Chrome 79 will NOT receive the new SameSite behavior.
- **Dec 19, 2019**: Chrome 80 Beta released. Experimental behavior still enabled for 50% of Chrome 80 Beta users.
- **February 4, 2020**: Chrome 80 Stable released. The enablement of the SameSite-by-default and SameSite=None-requires-Secure enforcement will not be included in this initial Chrome 80 stable rollout. Please see the next item for more detailed information on the when SameSite enforcement will be enabled for Chrome 80 stable.
- **February, 2020**: Enforcement rollout for Chrome 80 Stable: The SameSite-by-default and SameSite=None-requires-Secure behaviors will begin rolling out to Chrome 80 Stable for an initial limited population starting the week of February 17, 2020, excluding the US President's Day holiday on Monday. We will be closely monitoring and evaluating ecosystem impact from this initial limited phase through gradually increasing rollouts.
- **March 2, 2020**: The enablement of the SameSite enforcements has been increased beyond the initial population. However, it is still targeting an overall limited global population of users on Chrome 80 stable and newer. We continue to monitor metrics and ecosystem feedback via our tracking bug, and other support channels.

如果Smartbi 与第三方系统部署在不同的机器上，或者部署在同一机器不同的应用服务器域下，即出现跨域访问，就会导致在第三方系统通过iframe的方式集成Smartbi的资源，单点登录的时候获取不到对应的用户信息。

2. 为什么浏览器要做这方面的限制？

之所以谷歌浏览器会对进行这里集成限制，是从安全考虑的，因为如果不限制，第三方系统上外嵌的iframe可能会存在被设置成钓鱼网站的风险。

3. 对于相同版本的Chrome有些会有些不会的原因分析

以前的谷歌版本跨域是允许传递cookie的，但最近谷歌的新版本开始会有很多不允许跨域传递cookie的情况，所以开始出现问题。具体从哪个版本开始目前我们也不是很清楚，根据客户的反馈以及我们测试，大多是chrome 版本 80.0.3987.132（正式版本）会有不允许跨域传递cookie的情况。但不是所有人用这个版本都会有问题，谷歌采用灰度测试，即使是同版本，也是部分覆盖，部分不覆盖。且后续谷歌的新版本可能会一直存在不允许跨域传递cookie的情况。

解决方法

方案一（推荐）：

如果第三方集成系统本身是通过域名访问方式，因为本质是跨域问题导致的，可以先从域名/ip方面解决跨域的问题，如把smartbi服务器跟第三方系统集成环境的服务器加到一个域名/IP下解决跨域问题。

相关资料请查看：https://blog.csdn.net/yup1212/article/details/87633272

方案二（推荐）：

通过在第三方系统的应用服务器上**部署代理来解决跨域问题，即可解决本问题。（PS：在第三方系统所在机器上部署代理，设置代理服务器的IP和端口号和第三方系统保持一致，集成连接使用代理的集成地址，通过代理转发smartbi的请求，这样可以起到同源的作用）**

跨域问题解决文档：https://history.wiki.smartbi.com.cn/pages/viewpage.action?pageId=35750879

对于第三方系统是在Java应用服务器的，可以部署smartbi_proxy.war作为代理，对于第三方系统基于.net平台的，可以通过设置IIS来代理smartbi。

代理服务器部署方案：https://history.wiki.smartbi.com.cn/pages/viewpage.action?pageId=35750881

部署完代理后，访问第三方系统的地址和第三方系统集成的smartbi地址关系如下图：

适用情况：第三方系统的域较少。

特点：操作比较简单，风险较小，推荐使用。

方案三（推荐）：

通过部署第三方代理（例如Nginx等）来解决跨域问题，即可解决本问题。

适用情况：第三方系统的域较多。

特点：操作比较简单，风险较小，推荐使用。

nginx参考方案：nginx解决跨域问题方案参考

方案四：

由于目前发现部分谷歌浏览器80版本出现了这种问题，建议未升级到新版本的谷歌浏览器尽量不要升级到谷歌80版本，或者使用其他类型的浏览器，比如IE、火狐等（edge浏览器采用的是与Chrome浏览器相同的Webkit内核，也可能出现跨域）。

适用情况：第三方系统没有限制只能在谷歌浏览器上访问。

特点：操作比较简单，但是通用性差，无法控制用户访问的浏览器类型。

方案五（不推荐）：

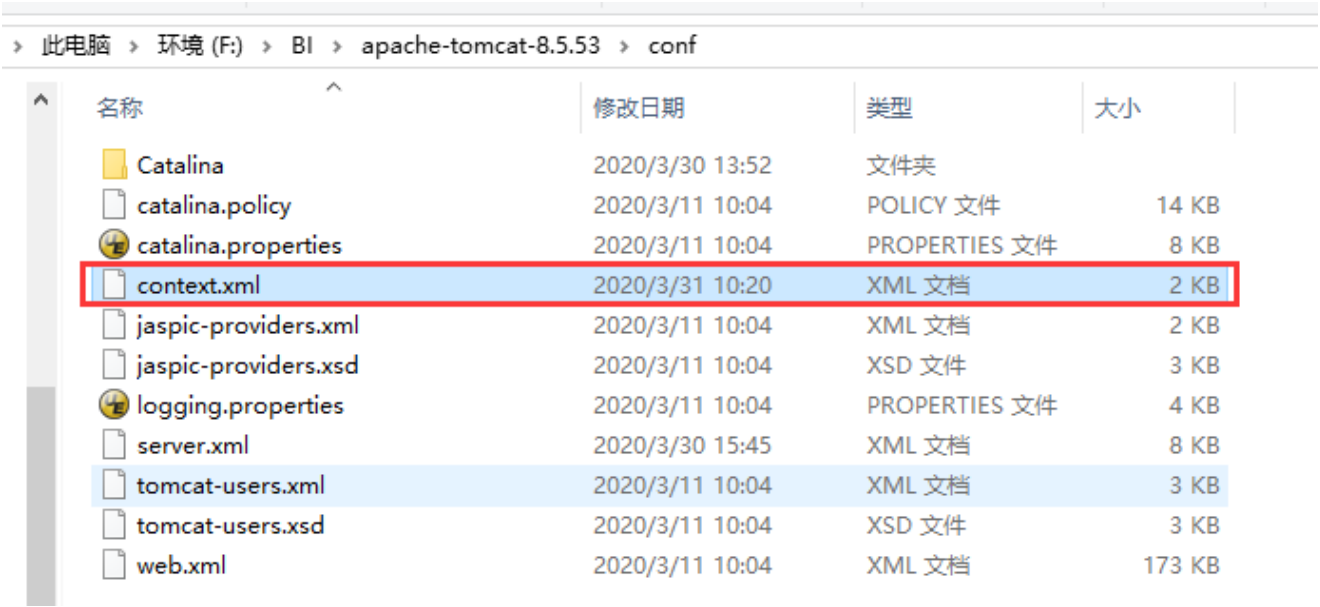
如果应用服务器是tomcat，Tomcat官方提供了通过升级tomcat到 8.5.53以上版本 ，修改 context.xml文件实现同源访问，具体请查看： http://tomcat.apache.org/tomcat-8.5-doc/config/cookie-processor.html ，**但必须要注意的是除了修改context.xml文件配置外，还要求应用服务器配置https协议。**

对于要求【应用服务器配置成https协议】可参考网上的一些资料分析，如：https://blog.csdn.net/Haran_ing/article/details/104337765

在Chrome 80中，Chrome会将没有声明SameSite值的cookie默认设置为SameSite=Lax。只有采用SameSite=None; Secure设置的cookie可以从外部访问，前提是通过安全连接(即HTTPS)访问。

本地验证此方案结果如下：

1、本地部署Tomcat8.5.53，找到： Tomcat\conf\context.xml 文件



2、对context.xml文件添加 ：<CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" sameSiteCookies="none" />

new 2 | context.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- The contents of this file will be loaded for each web application -->
<Context>

    <!-- Default set of monitored resources. If one of these changes, the    -->
    <!-- web application will be reloaded.                                   -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
    <CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" sameSiteCookies="none" />

    <!-- Uncomment this to disable session persistence across Tomcat restarts -->
    <!--
    <Manager pathname="" />
    -->
</Context>
```

3、部署smartbi的机器必须要配置成https方式，并且要求证书是浏览器受信证书，不受信的证书，Chrome浏览器也会拦截请求。配置https请查看wiki文档：https://history.wiki.smartbi.com.cn/pages/viewpage.action?pageId=35749900

4、为了避免因协议不匹配而造成一些功能不能正常使用，对于集成smartbi的第三方系统也需要配置成https访问方式。

综上，满足以上步骤要求的情况下，**通过升级Tomcat为8.5.53以上的版本配置context.xml文件并且smartbi及第三方集成系统都配置https访问方式（使用的浏览器受信的证书）**，本地验证可解决跨域访问问题。

另外如果是集群环境，集群环境是使用smartbi_proxy.war作为分发服务器的，smartbi_proxy.war所在Tomcat服务器也需要升级到Tomcat8.5.53版本以上，并且配置成受信证书的https访问方式，为了避免因协议不匹配集成环境也需要配置成https访问。

适用场景：应用服务器为tomcat， 并且传输协议为https。

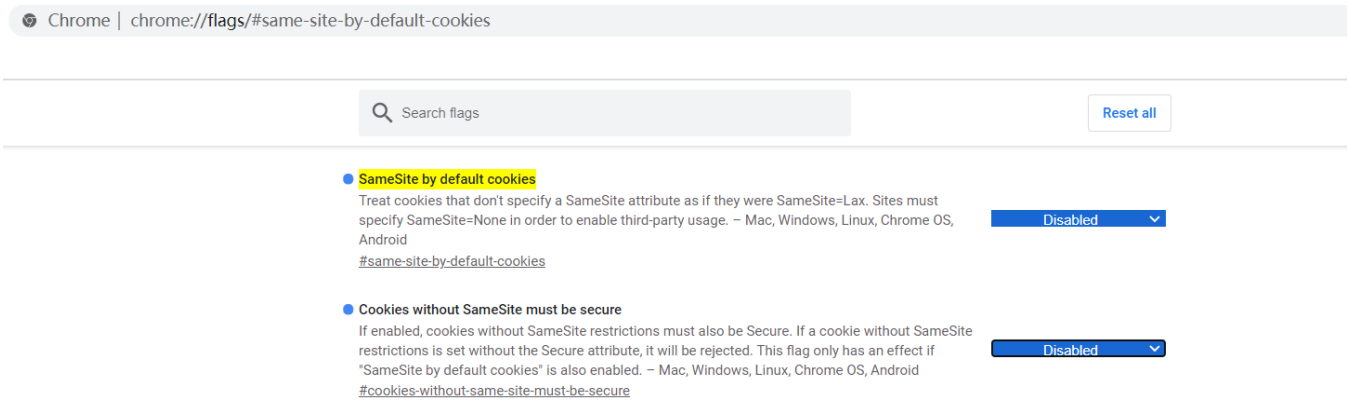
特点：通用性差（比如应用服务器非tomcat）；高版本tomcat要改较多的配置，比较麻烦，否则参数传递可能会失败；需要部署https证书（多个域需要多个证书），存在未知风险，不推荐使用。

注意：Tomcat版本的更新，对于安全性要求越来越高，高版本Tomcat目前已知的集成访问问题请查看wiki文档：Tomcat高版本部署smartbi通过URL拼接参数打开报表报400

方案六：

1.打开chrome 浏览器
2.地址栏输入chrome://flags/#same-site-by-default-cookies
3.分别把same-site-by-default-cookies 和 cookies-without-same-site-must-be-secure 设置为Disabled
4.然后重启浏览器

注：chrome 91及以上版本做了修改，不适用chrome 91及以上版本。



Viewtracker License Missing

There is a problem with the license of the Viewtracker addon. Please check if you have a valid license.

授权码细节