SSO & AZure AD 集成前期研究文档

# 参考内容

研究过程中参考了如下几个产品的SSO/Azure AD 集成的实现方式

1. Zendesk 的SSO 集成
2. LiveChatInc 的SSO 集成
3. Salesforce 的Azure AD 集成

总体而言，Zendesk 的集成方式是最值得借鉴的, 但是因为我们的产品不像Zendesk 这样每个站点都有自己的独立域名, 所以具体的实现方式还是会有所区别。

# 研究内容

## **Zendesk 的SSO 集成**

Zendesk 支持SAML2 和JWT 两种协议。因为Azure AD 本身就支持SAML2 , 所以不再提供单独的Azure AD 集成功能。Zendesk 官方也提供了文档用于说明如何把Azure AD 通过SAML2 协议集成到Zendesk 产品。

默认情况下，即使选择启用SSO 功能，用户还是可以通过Zendesk 的账号来登录系统, 登录的地址是[https://\*\*\*.zendesk.com/access/normal](https://***.zendesk.com/access/normal) ，但是如果访问常规的登录地址[https://\*\*\*.zendesk.com/Agent](https://***.zendesk.com/Agent) 则会直接跳转到SSO 的登录界面。输入正确的账号密码并验证成功后，就会直接进入Zendesk 的功能界面。

Zendesk 提供了一个选项: Disable Password, 如果此选项被勾选, 则只能通过SSO的方式登录，24小时内，Zendesk 账号的密码会被删除，但是官方不推荐使用这种方式。

通过测试发现, Zendesk 和IDP 的账号是通过Email 关联起来的。如果Email 对应的账号在Zendesk 中不存在，是不会自动在Zendesk 创建一个新账号的。

Zendesk 的SSO 集成是支持手机客户端的.

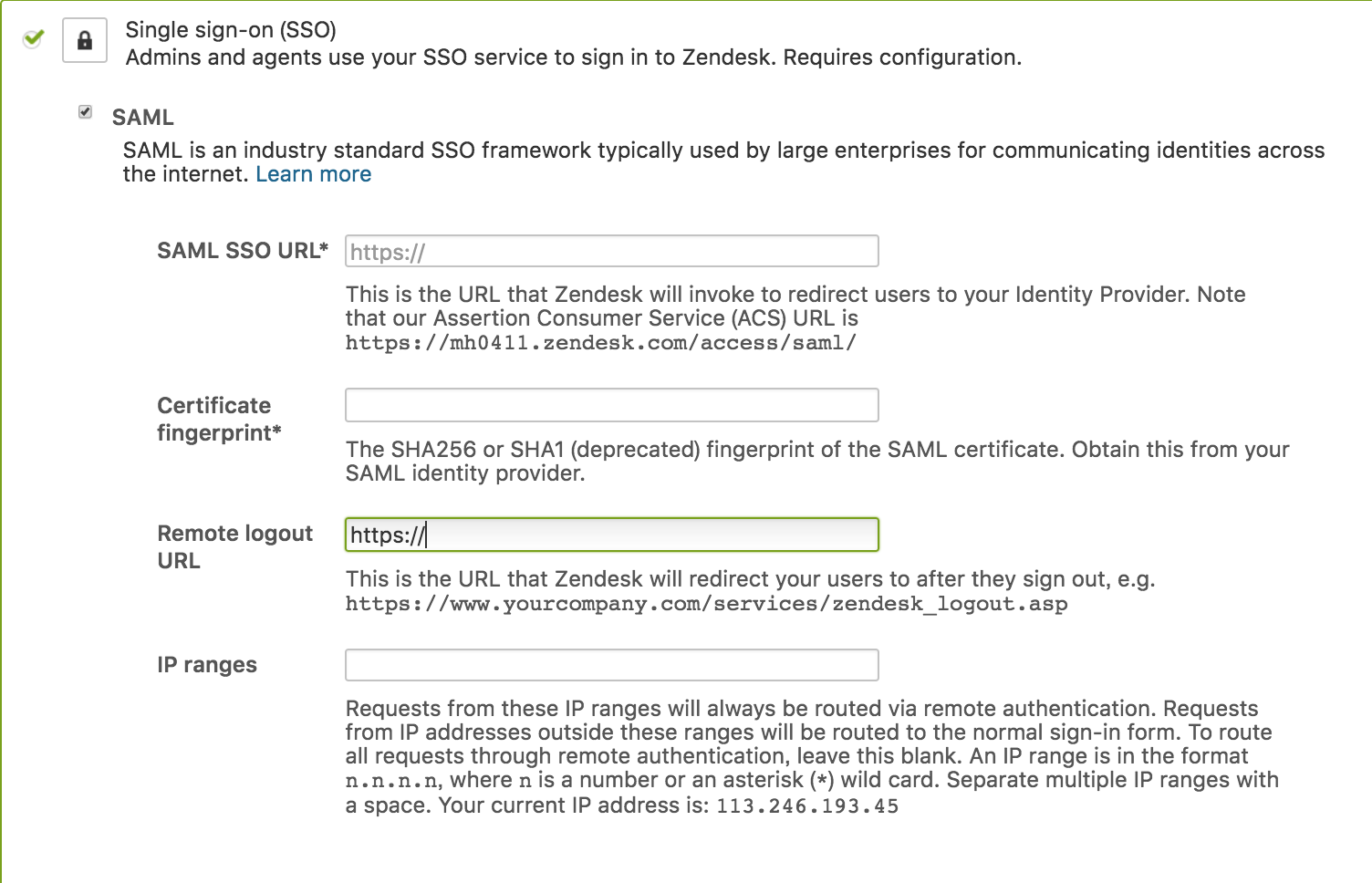


图2.1 SAML 的配置界面

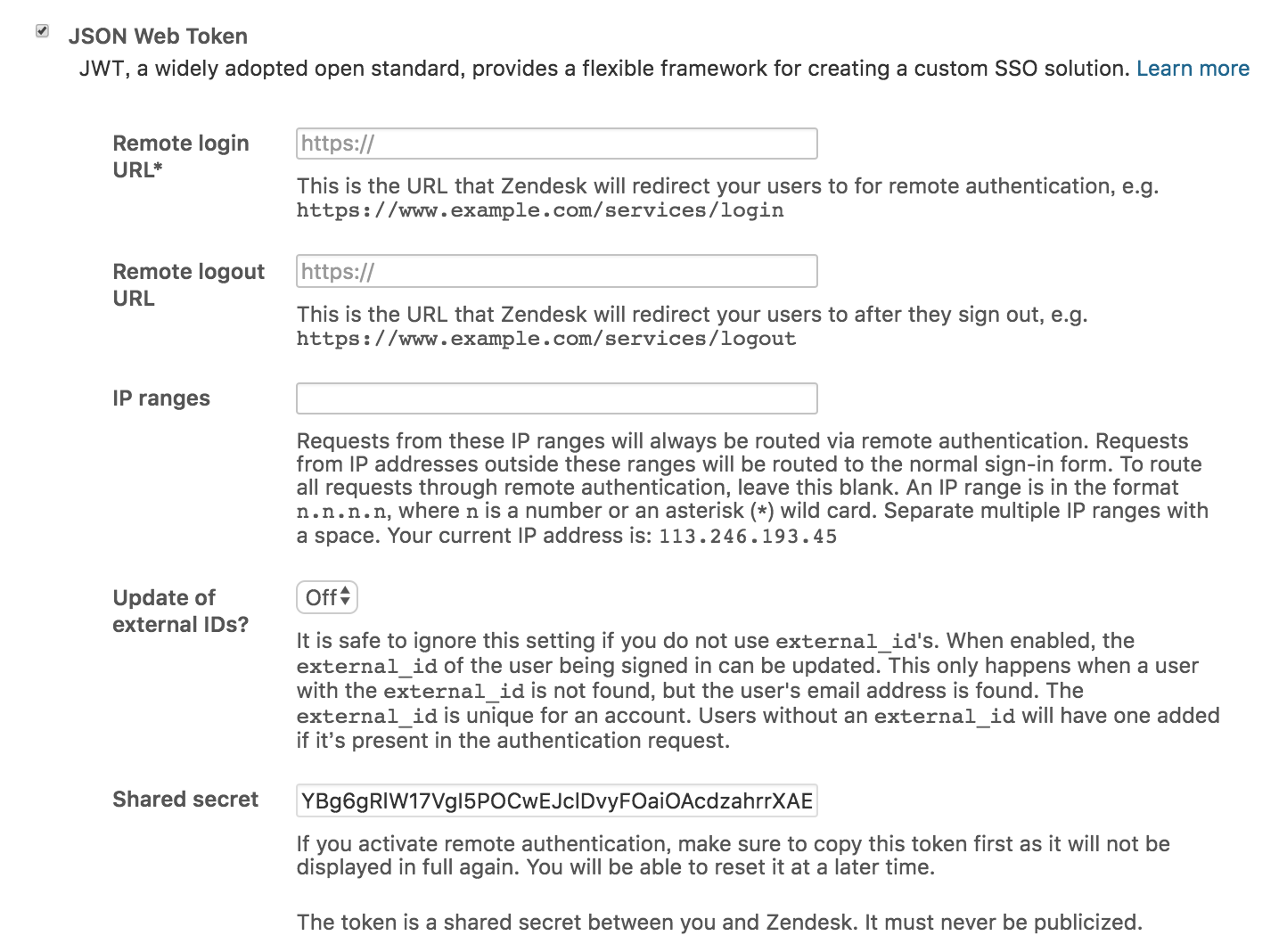


图2.2 JWT的配置界面

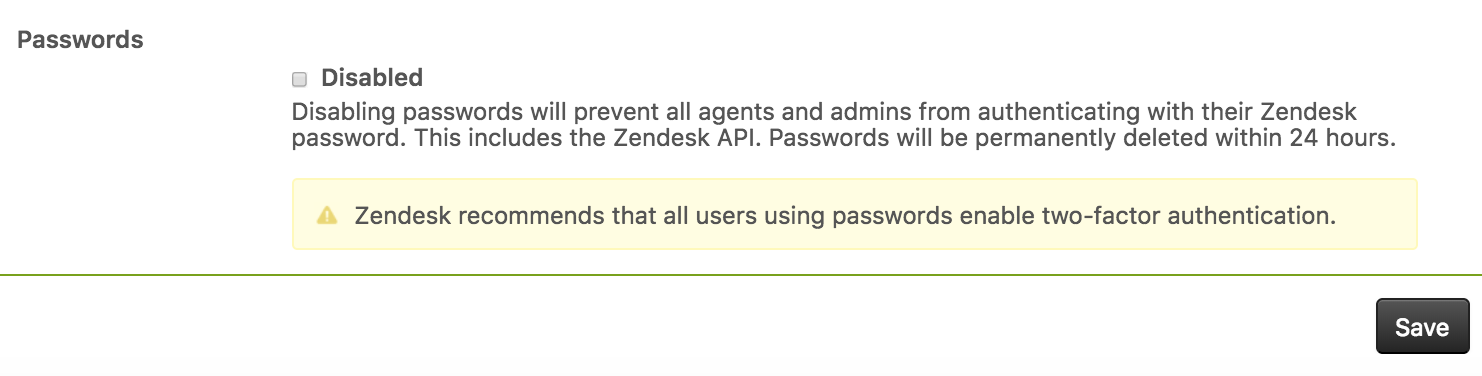


图2.3 Disable Password

如果是要把Azure AD 通过SAML 协议集成到Zendesk, 除了Zendesk端的基本配置外，企业还需要做如下几个事:

1. 把自己的Azure AD 配置成支持SAML2.0
2. 登录Azure , 到App Store 里面安装Zendesk 的SSO 集成Application
3. 进入Zendesk 的Application 选择需要启用Zendesk SSO 功能的 Azure AD 账号 ，点击[Assign] 按钮，完成匹配。

对应文档的地址是: <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-zendesk-tutorial>

## **LiveChatInc的SSO 集成**

LiveChatInc 只支持SAML2.0 , 因为只有收费账号才有SSO 的功能，所以信息均来源于官方文档，没有进行过实际操作。

因为LiveChatInc 的每个客户是没有自己的独立域名的，所以需要先在LiveChatInc 自己的登录页面输入邮箱地址（用于判定该用户属于哪一个站点），password 不填，点击登录后才会跳转到客户配置的SSO的登录界面。一旦启用了SSO 功能，用户就再也不能通过原来的LiveChatInc 的账号密码来登录系统了。启动SSO 功能后，LiveChatInc 会给所有的Agent 发一封邮件，告知不能再通过原来的账号密码进行登录。

对应文档的地址是: <https://www.livechatinc.com/kb/setting-up-sso-as-a-login-method/>

## **Salesforce的Azure AD集成**

Salesforce 的Azure AD 集成是Sam 演示给我看的，基本流程和Zendesk 非常相似, 用户也需要注册一个已经上传到Azure 的Salesforce Application, 然后在Application 和Salesforce 2端都进行一些配置才能使用Azure AD 账号登录Salesforce.

Salesforce 会在登录界面添加一个使用SSO 进行登录的按钮，点击该按钮进入Azure AD 集成的登录界面。也就是说，用户可以在 Salesforce账号密码登录/和Azure AD 登录 之间进行选择。

配置的方式: <https://docs.microsoft.com/zh-cn/azure/active-directory/active-directory-saas-salesforce-tutorial>

## **总结**

通过以上的研究，我的总体思路是:

1. 我们的SSO 只支持SAML 协议, （JWT 用的比较少，是否支持可以再讨论）, Azure AD 也通过SAML 协议来进行集成，不提供单独的Azure AD 集成功能.
2. SSO 集成功能的开启是针对站点级别的，一旦开启了，普通的账号/密码登录的方式就不提供了，开启此功能时可以像LiveChatInc 一样给所有用户发一封邮件。
3. 用户登录Portal 时，需要先输入邮箱地址(密码可以不填)，点击登录，我们的系统才能通过邮箱确定具体调到哪个IDP 提供的登录界面。
4. 如果是直接登录Agent Console , 因为链接地址是带了Site Id 的，我们可以直接跳转到对应IDP 提供的登录界面。
5. 既然Zendesk 可以支持手机客户端的SSO 登录，我们应该也可以实现, 现在看上去是通过用嵌入式窗口来加载登录界面的，我们的系统也应该支持手机客户端的SSO 登录功能。