### SSO Requirement

#### 总体说明

SSO（Single Sign On）即单点登录。SSO是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

SSO项目内容包括：

1. 在Portal中开启单点登录功能并配置SSO参数。
2. 支持的产品有Portal、Agent Console（包括网站、手机端和桌面端）
3. 支持的协议包括SAML 2.0和JWT（JSON Web Token）
4. Azure AD集成通过发布Comm100企业应用到Azure AD application gallery list
5. 编写文档指导客户配置Portal及IdP/ JWT Authentication Server。

#### 总体流程图

图 1 总体流程图

#### 节点说明

##### 1.1 SSO Configuration

1) Portal的Settings菜单下新增一个页面Agent Single Sign-On，默认SSO未开启。该功能只有企业版拥有，如下图所示：

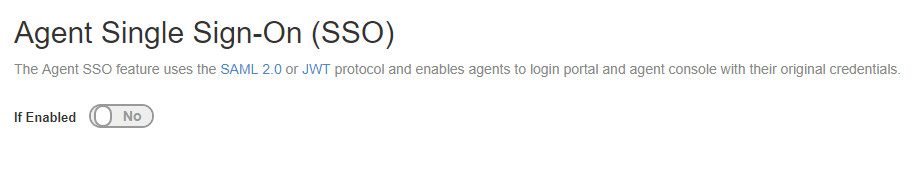


图 2 Agent SSO Disabled

2）点击If Enabled的Switch，开启Agent SSO功能。可以选择SAML或JWT协议，默认选中SAML Based Single Sign-On，如下图所示：



图 3 Enable Agent SSO and SAML SSO Settings

1. 开启成功后提示Agent Single Sign-On(SSO) enabled successfully.
2. SAML SSO URL必填，否则提示：SAML SSO URL is required.
3. SAML SSO URL必须以https://开头，否则提示：SAML SSO URL should use HTTPS.
4. Certificate必填，否则提示：Certificate is required.
5. Certificate格式必须正确（base64编码），否则提示：Invalid certificate. Please get the base64 encoded certificate from the Identity Provider.
6. Remote Logout URL验证参考SAML SSO URL。

3）点击JWT Based Single Sign-On，可以切换SSO协议为JWT，如下图所示：

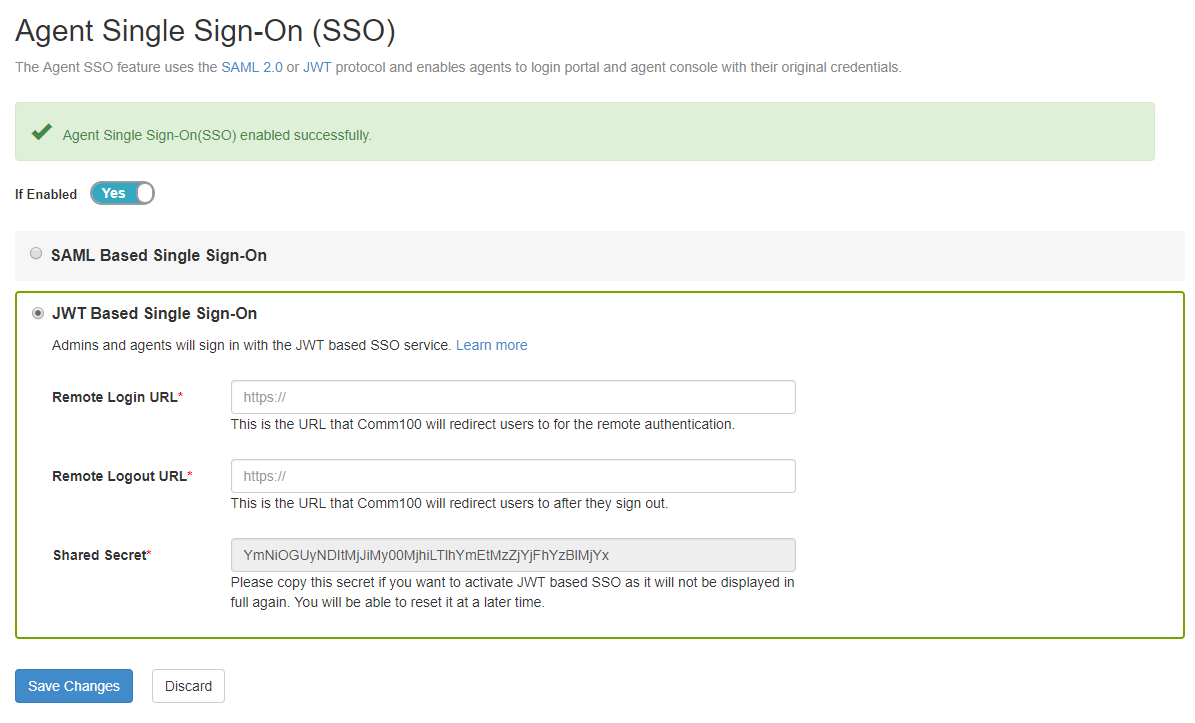


图 4 JWT SSO Settings

1. Remote Login URL及Remote Logout URL的字段验证同SAML SSO URL。
2. Shared Secret字段在当前还不是JWT SSO方式但是选中了JWT Radio时完整显示。当保存基于JWT的SSO配置后，再查看该字段只显示前8个字符，后面的字符隐藏，此时可以Reset。Reset成功之后显示完整的Secret以便用户复制，但是必须点击Save按钮后新的secret才会保存并生效。

4）当用户enable了Agent SSO且设置一种协议首次保存成功后，系统会向该站点所有Agent发送邮件，告知已开启SSO并附带详细使用说明。

5）当SSO开启并保存配置成功后，用户依然可以使用原来的Comm100用户和密码方式登录。如果是通过SSO自动添加的用户，系统会生成随机密码。

##### 1.2 Single Sign On

###### 1.2.1 确定Site 的规则

不同站点配置的IdP 是不同的, 因此要先确定siteId然后再根据siteId来确定对应站点是否启用了agent SSO 功能，如果是启用状态就根据具体的IdP配置来进行登录。

具体有如下几种情况:

1. 客户通过带siteId的URL 地址来登录, siteId 可以直接从URL里面取。

e.g. <https://ent.comm100.com/adminmanage/login.aspx?siteId=1000007>

(2) 客户通过不带siteId 的URL 地址登录, 这种情况下需要在登录页面选择[Sign in With agent SSO]，然后在下一步输入具体的siteId。Desktop 和mobile 版的Agent Console 也是这种处理方式。

(3）如果用户已经使用SSO登录过，系统会在浏览器Cookie 或者App 中存储对应的siteId并视情况进行更新。可以通过存储的siteId 来确定具体的站点。

三种方式的优先级是 (1) > (3) > (2)

如果用户通过带siteId 的URL地址登录，以URL中的siteId 为准，在SSO登录成功后会更新cookie 或app 中存储的siteId。如果用户通过不带siteId的URL 地址登录或直接进入Desktop 和mobile 版的Agent Console, 会先检测cookie 或app中是否存储了siteId, 如果已存储则直接使用这个siteId。

###### 1.2.2 SSO 登录总体流程

登录的方式比较多，具体的有

1. <https://www.comm100.com/secure/login.aspx> 登录 可以带siteId或不带siteId
2. [https://\*\*.comm100.com/adminmanage/Login.aspx](https://hosted.comm100.com/adminmanage/Login.aspx) 登录 可以带siteId或不带siteId
3. 登录portal 以后点击Get Online & Chat 自动登录到Web 版Agent Console
4. Web 版Agent Console 登录
5. Desktop 和Mobile 版登录

虽然方式多样，但SSO 的总体流程是相同的，具体来说，可以分为如下几步:

1. 用户进行登录操作
2. 系统接收到登录请求，判断siteId, 根据siteId 确定是否要使用SSO登录，如果需要使用SSO 登录，调用对应的IdP 服务，如果该Idp 下有Account 已在当前浏览器处于登录状态（存在对应的Session）会自动使用该账号登录，否则，用户需要输入账号密码进行验证。
3. SSO 验证通过后，Comm100 系统还需要验证对应站点中是否存在一个有效的Account 它的邮箱地址和SSO Account 的邮箱地址相同，验证通过后，成功登录Comm100 系统。

如果不需要用户自己输入siteId 并且有SSO 帐号当前正处于登录状态，用户在访问登录地址或登录app 时不需要再输入任何帐号信息会直接成功登录Comm100系统。

以下分不同产品对用户使用SSO功能的流程进行描述。以SAML为例，JWT流程类似。

###### 1.2.1 Portal SSO

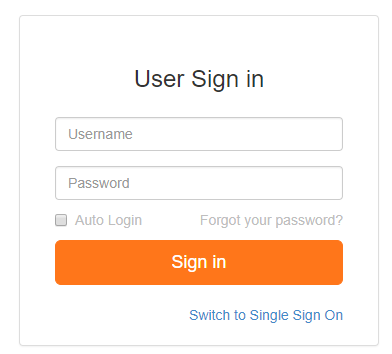
1) 用户进入Portal登录页面，默认显示Comm100账号认证界面及切换到SSO的链接，如下图所示：

图 5 Portal Comm100 Account Login

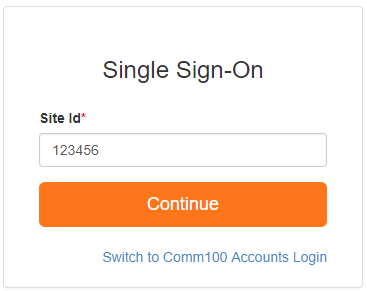
2）用户点击“Switch to Single Sign On”链接，显示下图所示SSO界面：

图 6 Portal Single Sign-On

1. 用户点击Switch to Single Sign On及Switch to Comm100 Accounts Login链接时，浏览器会记录用户最后一次的使用状态。下次进入登录界面时自动显示相应界面。
2. 点击Continue时会将Site Id缓存。如果查询参数中没有附带Site Id，且Site Id缓存不为空，则将其初始化为Site Id的值。
3. Site Id必填，否则提示：Site Id is required.
4. Site Id必须为正整数，否则提示：Site Id should be a positive integer.
5. 如果该站点未开启SSO或SSO未配置，则提示：SSO has not been enabled or configured for this site.

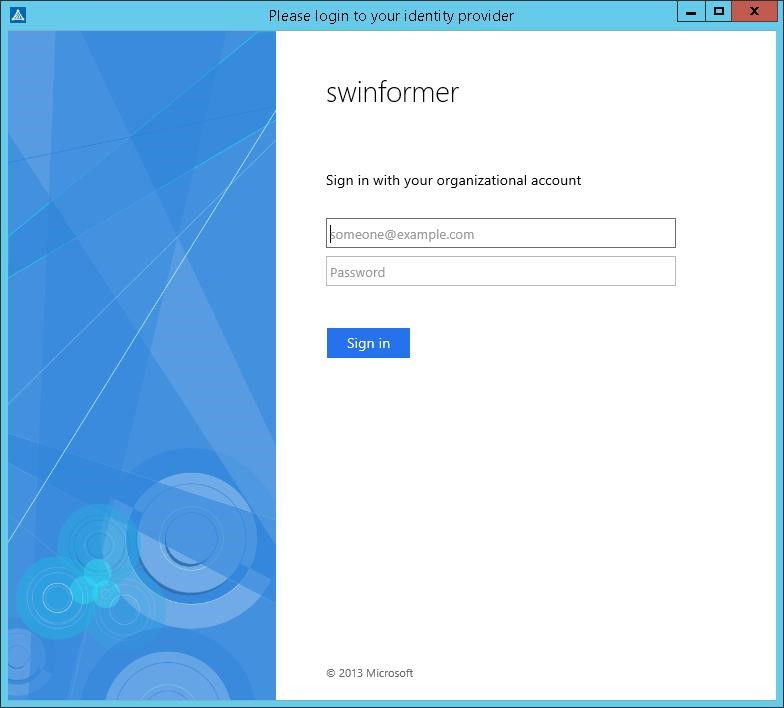
3) 用户输入Site Id, 点击Continue按钮，浏览器跳转到IdP登录页面，如下图所示：

图 7 IdP Login Page

4) 输入用户名（邮箱地址）和密码，点击Sign in按钮，认证成功后跳转到Portal页面，如下图所示：

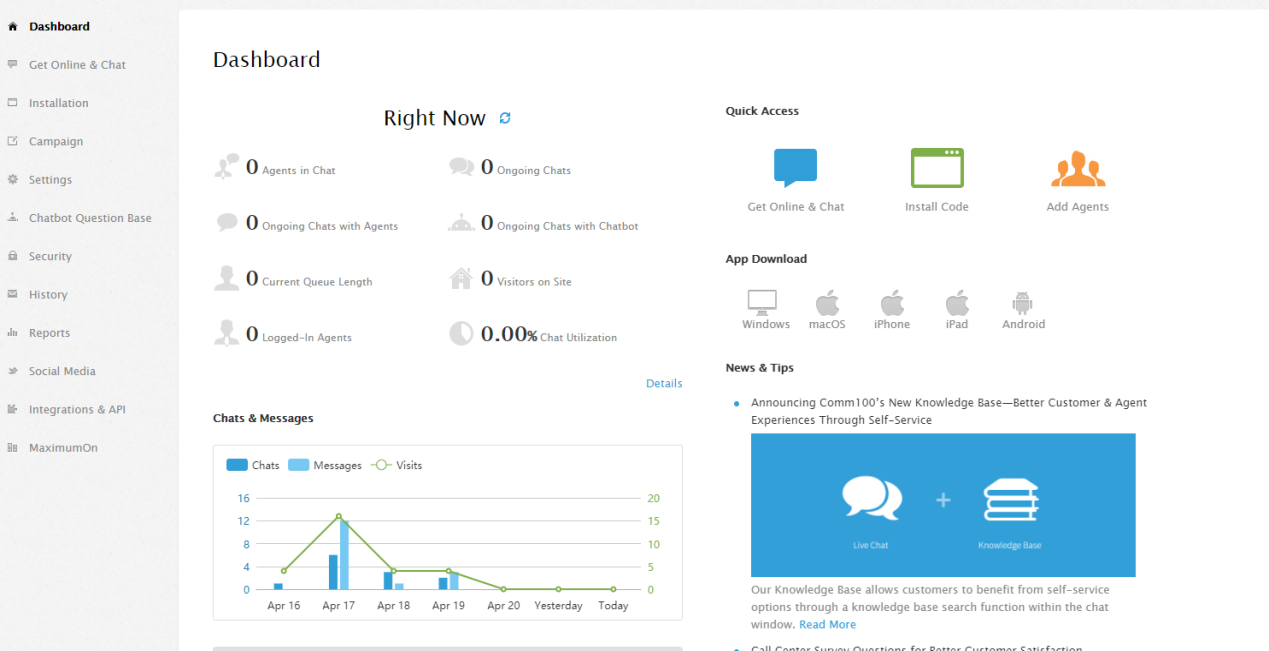


图 8 Portal Dashboard

5) 如果IdP之前登录过，用户未Logout且IdP Session还没过期，则3)中用户会跳过输入用户名密码的步骤而自动以IdP Session中保存的用户登录。

6）如果用户是在访问其他页面因为Session过期等原因跳转到登录页面，查询参数中附带有跳转目标地址，则IdP认证通过后浏览器跳转回该目标地址。

7）IdP认证成功后返回的用户邮箱地址如果在Comm100中不存在，则将其添加到登录指定Site Id下；如果返回的邮箱地址在Comm100中存在且其Site Id与登录指定Site Id一致，则登录成功；如果返回的邮箱地址在Comm100中存在但其Site Id与登录指定的Site Id不一致，则登录失败，返回登录页面且提示失败原因。

###### 1.2.2 Agent Console Website/Desktop SSO

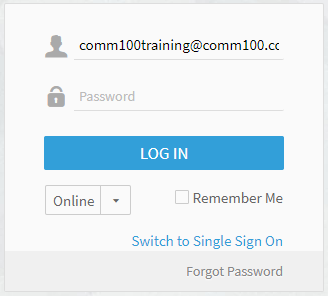
1) 进入Agent Console登录页面，默认显示Comm100账号认证界面及切换到SSO的链接，如下图所示：

图 9 Agent Console Website Comm100 Accounts Login

2）点击Switch to Single Sign On链接，显示下图所示SSO界面：

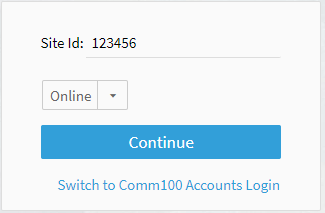


图 10 Agent Console Website SSO

1. 用户点击Switch to Single Sign On及Switch to Comm100 Accounts Login链接时，浏览器会记录用户最后一次的使用状态。下次进入登录界面时自动显示相应界面。
2. Site Id必填，否则提示：Site Id is required.
3. Site Id必须为正整数，否则提示：Site Id should be a positive integer.
4. 如果该站点未开启SSO或SSO未配置，则提示：SSO has not been enabled or configured for this site.

3) 输入Site Id，点击Continue按钮，浏览器跳转到IdP登录页面如前面图 7所示。

4）输入用户名密码，点击Sign in，认证成功后跳到Agent Console Visitors Tab，如下图:

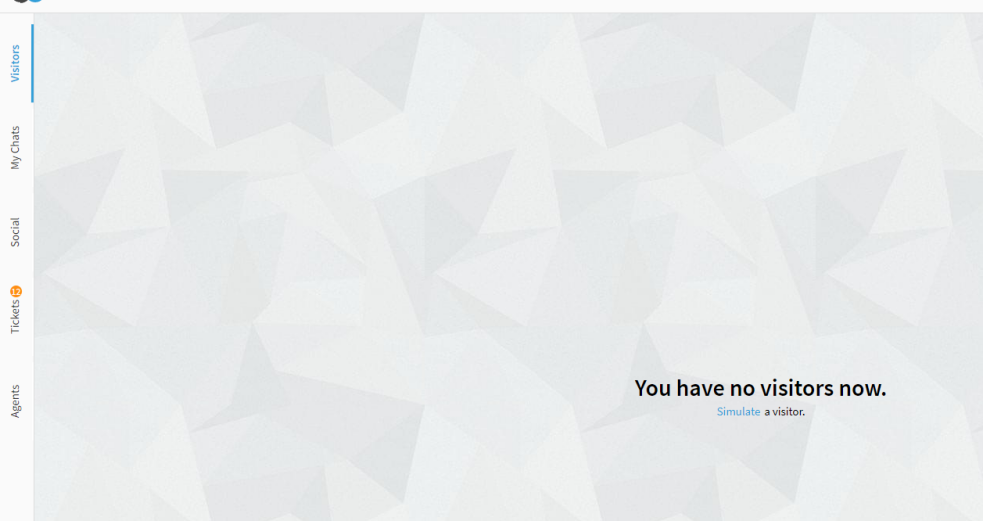


图 11 Agent Console Visitors Tab

5) 如果IdP之前登录过，用户未Logout且IdP Session还没过期，则3)中用户会跳过输入用户名密码的步骤而自动以IdP Session中保存的用户登录。

6）IdP认证成功后返回的用户邮箱地址如果在Comm100中不存在，则将其添加到登录指定Site Id下；如果返回的邮箱地址在Comm100中存在且其Site Id与登录指定Site Id一致，则登录成功；如果返回的邮箱地址在Comm100中存在但其Site Id与登录指定的Site Id不一致，则登录失败，返回登录页面且提示失败原因。

###### 1.2.3 Agent Console Mobile SSO

1）打开手机应用，进入下图所示登录页面：



图 12 Mobile app login page

2) 点击Switch to Single Sign On链接，显示下图所示SSO界面：



图 13 Mobile app SSO

3）输入Site Id，点击Continue，应用进入IdP登录页面，如下图所示：

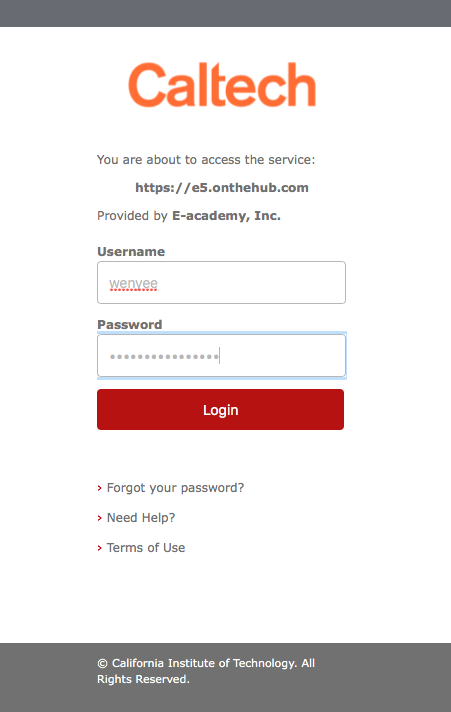


图 14 Mobile IdP Login Page

4）输入用户名密码在IdP认证通过后，手机端应用登录成功。

5）如果IdP之前登录过，用户未Logout且IdP Session还没过期，则3)中用户会跳过输入用户名密码的步骤而自动以IdP Session中保存的用户登录。

6）IdP认证成功后返回的用户邮箱地址如果在Comm100中不存在，则将其添加到登录指定Site Id下；如果返回的邮箱地址在Comm100中存在且其Site Id与登录指定Site Id一致，则登录成功；如果返回的邮箱地址在Comm100中存在但其Site Id与登录指定的Site Id不一致，则登录失败，返回登录页面且提示失败原因。

###### 1.2.4 SSO Auto Login

1）鉴于SSO的特殊性，首次点击Continue按钮后自动开启Auto Login。如此，用户下次进入登录页面时，不需要再次点击Continue按钮确认，而是会自动跳转到IdP登录页面，使流程更流畅。

2）Logout会关闭Auto Login。Logout后首次进入SSO Login需要再次点击Continue按钮。

3）如果目标地址附带查询参数SiteId及IsSSO（值为true），在登录页面编写逻辑自动获取Site Id并跳转到IdP登录页面，这样可以跳过第一次的点击Continue按钮过程。

##### 1.3 Single Logout（SLO）

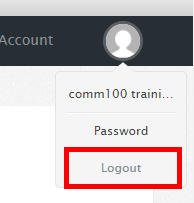
1）首先点击原有的注销按钮，清除Comm100自己的Session。

图 15 Portal Logout

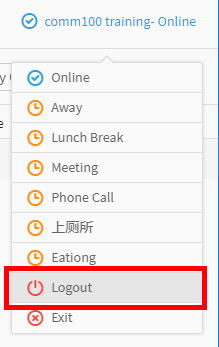


图 16 Agent Console Logout

2）Comm100注销后浏览器将跳转到Remote Logout URL自动清除IdP/JWT Authentication Server的Session。

**注意**：由于Desktop Agent Console的特殊性，当浏览器跳转到Remote Logout URL后请注意自动跳转回登录页面。