### SSO Requirement

#### 总体说明

只有企业版支持此功能.

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SSO帐号就可以访问所有相互信任的应用系统。

Agent SSO的功能内容包括：

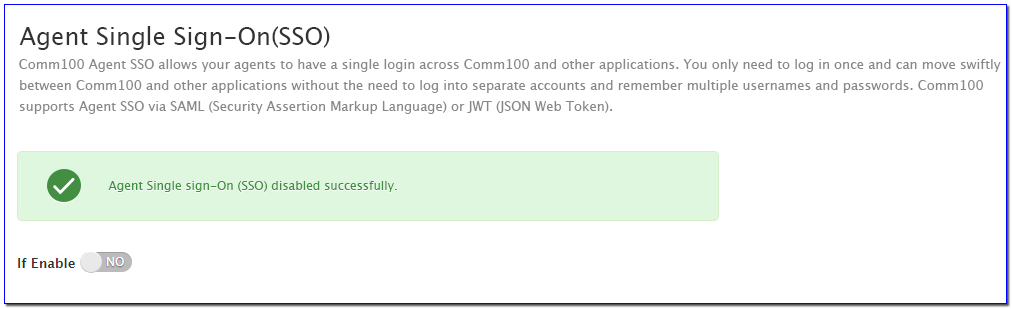
1. 在My Account中开启单点登录功能并配置相关参数。支持的协议包括SAML 2.0和JWT（JSON Web Token）, Azure AD 因为支持SAML 2.0 协议，所以可以直接集成。
2. 如果站点开启了Agent SSO 功能，用户可以使用SSO帐号登录Comm100 的系统.，如果SSO帐号已经处于登录状态则可以直接登录，不需要输入账号密码。

3. 提供Logout from SSO Account 功能，确保用户可以切换SSO帐号进行登录。

#### 功能说明

##### My Account ->Security->Agent Single Sign-On

* My Account的 Security菜单下新增一个页面Agent Single Sign-On



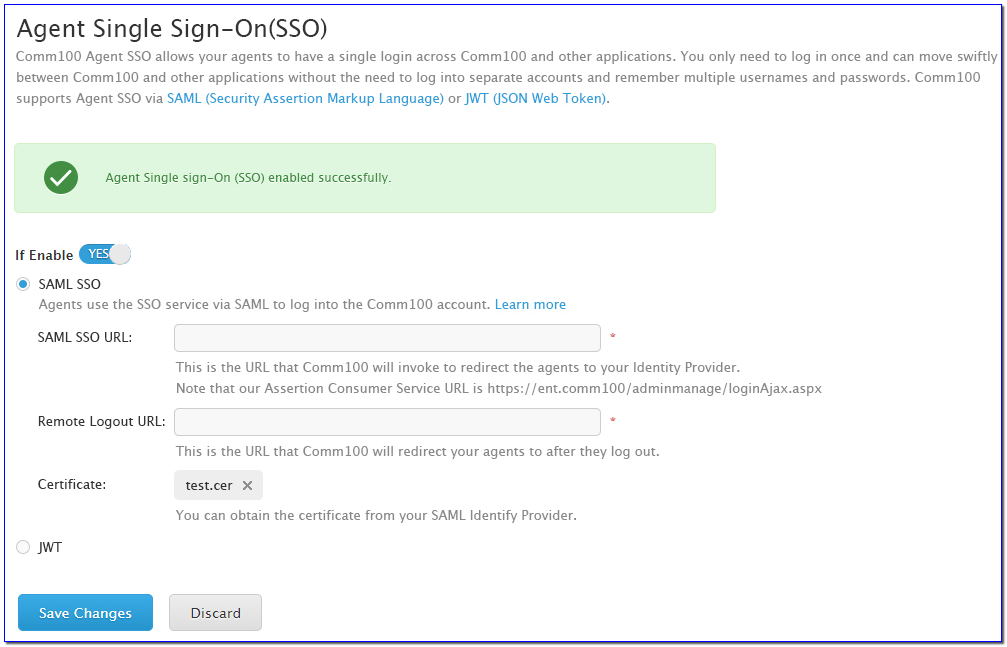
**业务规则:**

1. 该功能默认关闭. 开启时提示”Agent Single sign-On(SSO) enabled successfully.”

关闭时提示”Agent Single sign-On(SSO) disabled successfully.”

1. SAML(Security Assertion Markup Language) 和JWT(JSON Web Token) 是超链接, 链接地址是分别是<https://en.wikipedia.org/wiki/SAML> 和 <https://en.wikipedia.org/wiki/JWT> ，点击会在新窗口打开链接地址。

* 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 SSO URL，如下图所示：



**业务规则:**

1. SAML SSO URL 和Remote Logout URL 都是必填，否则提示”SAML SSO URL is required.”。
2. SAML SSO URL 和Remote Logout URL 都必须以https:// 开头, 否则提示URL should start with https://
3. Certificate必填，否则提示：Certificate is required.
4. 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.
5. Learn more 是一个超链接，对应的是一个KB 文章的地址(地址待定)

* 点击JWT ，可以切换SSO协议为JWT，如下图所示：

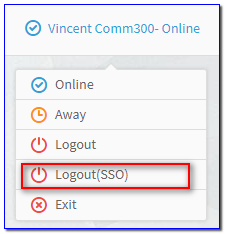


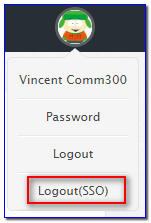
**业务规则:**

1. Remote Login URL及Remote Logout URL的字段验证同SAML SSO URL
2. Shared Secret 是只读的，在第一次开启SSO功能时会生成一个随机的Secret, 用户可以点击Reset 按钮重新生成新的Shared Secret.
3. Learn more 是一个超链接，对应的是一个KB 文章的地址(地址待定)

* 开启Agent SSO 功能后的对系统的影响

1. 只有管理员还可以继续使用Comm100 账号/密码登录系统，其它用户只能使用SSO 登录。
2. 除管理员外，其它用户均不能再使用reset password 功能.
3. 对应站点的portal 、Agent Console 均会多一个“Logout(SSO)”选项





##### 2.2 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SSO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 直接从URL里面取。

e.g. [https://ent.comm100.com/adminmanage/login.aspx?](https://ent.comm100.com/adminmanage/login.aspx?siteId=1000007)**[siteId](https://ent.comm100.com/adminmanage/login.aspx?siteId=1000007)**[=1000007](https://ent.comm100.com/adminmanage/login.aspx?siteId=1000007)

(2) 如果用户已经使用SSO成功登录过，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。此时可以通过存储的siteId 来确定具体的站点。

(3) 客户通过不带siteId 的URL 地址或登录desktop/mobile版Agent Console时，会先检测cookie 或APP是否存储了siteId, 如果未存储则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。

三种方式的优先级是 (1) > (2) > (3)

###### 1.2.2 SSO 登录总体流程

具体来说，可以分为如下几步:

1. 用户进行登录操作(访问登录地址、进入Comm100 app..)
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 登录当对应的SSO System 下有Account 已在当前浏览器处于登录状态时（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。

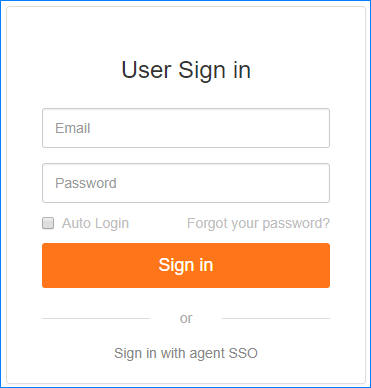
如果不需要用户自己输入siteId 并且有SSO 帐号当前正处于登录状态，用户在访问登录地址或登录app 时不需要输入任何帐号信息直接成功登录Comm100系统。

###### 1.2.3 Portal SSO

Portal 有如下2种登录方式:

1. 访问地址 <https://www.comm100.com/secure/login.aspx>
2. 访问地址 [https://\*\*\*(ent or hosted) .comm100.com/adminmanage/Login.aspx](https://ent.comm100.com/adminmanage/Login.aspx)
3. 如果是通过带siteId 参数的URL地址登录， 当对应站点开启了Agent SSO 功能时会自动跳过普通登录界面直接进入SSO 登录流程。如Agent SSO 功能未开启，则还是使用普通的登录方式。
4. 如果是通过不带siteId 参数的URL 地址登录, 需要点击[Sign in with agent SSO] 来确定使用SSO 进行登录。如果cookie 中存储了siteId，输入siteId 这一步骤会自动跳过。

*Note:* 这一点上portal 和Agent Console 的处理方式是不同的，Agent Console 只要检测到cookie 或app 中存在siteId 并且对应站点开启了Agent SSO功能就会自动进入SSO 登录流程。portal 采用这种处理方式的原因是SSO 的配置可能进行过错误的修改导致无法使用SSO帐号进行登录，如果管理员不能手动选择登录方式就无法进入系统修改SSO的配置





**业务规则**

1. Site Id必填，否则提示：Site Id is required.
2. Site Id必须在系统中存在，否则提示：This site Id does not exist.
3. 如果该站点未开启SSO，则提示：Agent SSO feature has not been enabled.
4. 用户可以点击<<go back 回到普通登录页面。
5. 输入的Site Id有效，点击[Next]
6. 如果已经有SSO 账号在当前浏览器处于登录状态，并且对应站点存在一个有效用户和SSO账号的email 相同，直接登录portal
7. 如果没有SSO账号在当前浏览器中处于登录状态, 需要用户在SSO登录界面输入账号密码进行验证，如果对应站点存在一个有效用户和用户输入的SSO账号的email 相同，则成功登录portal.

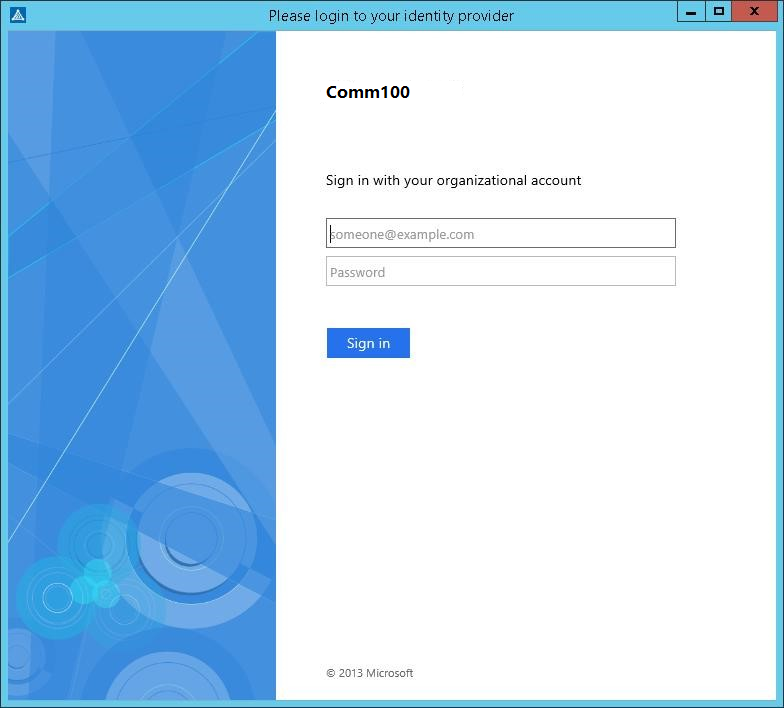


图: 进入SSO 的登录界面进行验证

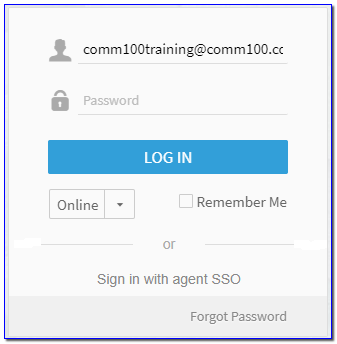
1. 如果用户通过SSO 账号登录portal 成功，会更新cookie 的siteId

###### 1.2.4 Web/Desktop版 Agent Console SSO

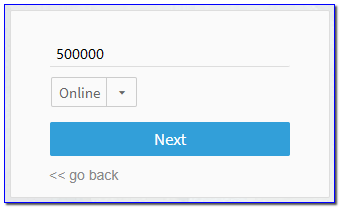
1. Web 版的Agent Console 是通过URL 地址访问的，所以可以通过URL 地址来获取siteId。

2. 如果URL 中没有带siteId 参数或使用的是Desktop版, 但是Cookie 中存储了siteId 而且对应站点也开启了Agent SSO 功能，会默认使用SSO 的方式登录系统.

3. 成功使用SSO 方式登录Agent Console 后会自动更新浏览器cookie 中的siteId, 减少下次登录时的不必要操作。



图Web/Desktop 版的Agent Console登录界面



图Web/Desktop 输入站点界面

（4）其它的业务规则和Portal SSO 是相同的，此处不在复述.

###### 1.2.5 Mobile 版Agent Console SSO

###### 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：

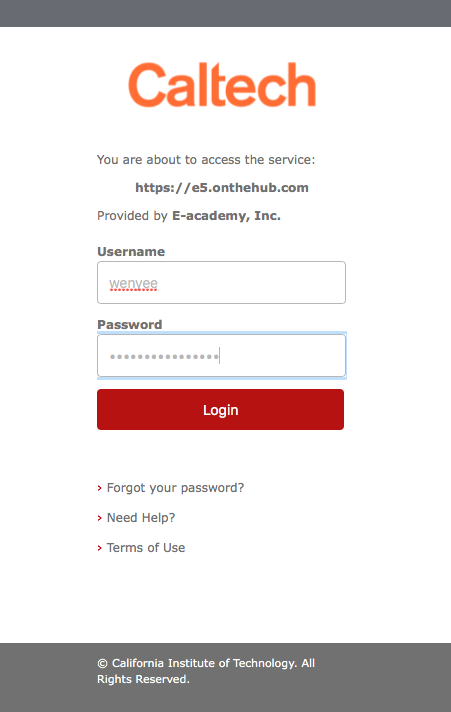


图 14 Mobile IdP Login Page

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）

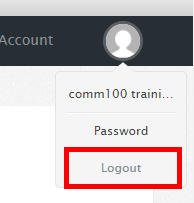
1）首先点击原有的注销按钮，清除Comm100自己的Session。

图 15 Portal Logout

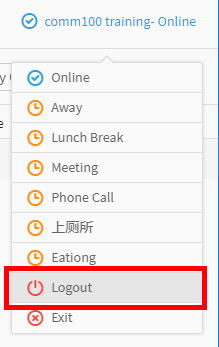


图 16 Agent Console Logout

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。