Single Sign-on with CAS

Agiloft supports single sign-on on the web via integration with Apereo CAS (Central Authentication Server). This allows Agiloft to have integrated authentication with products such as uPortal, BlueSocket, TikiWiki, Mule, Liferay, Moodle, and others.

From the user's point of view, the typical integrated scenario is simple. First, they log in to a CAS-enabled product such as uPortal. Then, using a hyperlink from within the portal, the user can easily access the Agiloft system. When Single Sign On via CAS is enabled, you can also configured outbound emails so that any hotlinks that they contain use CAS to authenticate the user and access Agiloft.

Technical Overview

For the typical integrated scenario described above, the following occurs:

1. When the user logs in to the CAS-enabled product, CAS issues a secure token that is usually stored as a cookie.
2. When the user presses the hyperlink to access Agiloft from within the portal, Agiloft uses a client-side redirect to pass the URL contained within the hyperlink to CAS. Note that this is the same process that occurs if the user selects a CAS-aware hotlink from within an email they received from the Agiloft system.
    a. If the user is currently logged in to CAS, CAS verifies the token and redirects the user back to the URL within Agiloft. The location of the Agiloft instance is determined automatically at installation time or overridden when the Hotlink Server Root URL global variable is passed to CAS to tell it where to find the Agiloft instance after authentication is performed.
    b. If the user hasn't logged in to CAS or CAS requires reauthentication, then CAS displays a login form, authenticates the user, and, if successful, performs a client-side redirect back to the URL within Agiloft. As above, the location of the Agiloft instance is determined automatically at installation time or overridden when the Hotlink Server Root URL global variable is passed to CAS to tell it where to find the Agiloft instance after authentication is performed.
3. When CAS sends the user back to the original URL, the redirect contains another secure token that confirms that authentication has been performed. After verifying the authenticity of the secure token, Agiloft obtains the username via direct connection to CAS and logs in.

Note that the hyperlink embedded within the CAS-enabled portal follows the usual rules for Agiloft hyperlinks but uses a special entry point/cas-login and has no user and password credentials specified.

Example

```
<a href="http://example.agiloft.com/gui2/cas-login?
keyID=0&project=Demo&state=Main">http://example.agiloft.com/gui2/login.jsp?
keyID=&project=Demo&state=Main</a>
```

The structure of the URL output is: `https://AGILOFT_HOST/gui2/cas-login?KB_NAME&state=main`

For Agiloft hyperlinks, see Hyperlinks.

Setup

To configure Single Sign-on with CAS, complete the following steps on a per-KB basis:

1. Click the **Setup** gear in the top-right corner and go to **System > Manage Global Variables**.
2. Edit the CAS Server Login URL global variable so that it contains the URL where your CAS is located. For example, https://{yourhost}/cas/login.
3. Confirm that the CAS Ticket Validator global variable contains the correct CAS Server version available in your setup. If it doesn't, edit it so that it does.
4. If you wish to enable CAS-aware hotlinks in emails, edit the Hotlink Type global variable so that it has a value of CAS.
5. Embed a correctly formatted hyperlink to Agiloft within your CAS-enabled product.

Force SSO Login

Finally, to make sure users log in with SSO after the transition, manually set new passwords for users who should use SSO instead. To do so:

1. Go to the People table and select every user who should use SSO from this point on.

   > ✓ Don't select every single user in your system. It's best to leave at least one administrator unchanged, if not the whole admin team, in case you encounter SSO issues in the future that prevent users from logging in with SSO.

2. Click Mass Edit, or Edit Fields, in the action bar.
3. Select the Password field, then click Next to proceed to the Update tab.
4. Select the formula option and enter random_password(15). This will call the random_password(15) function to randomly generate a new 15-character password for everyone you selected.
5. Click Next, then Finish.
6. Now, go to Setup Employees and go to the Layout tab. If you will use SSO for every user in the system, including external users, go to Setup People instead.
7. Remove the Password field from the layout. This prevents users from manually setting a new password and potentially using it to log in instead of SSO.

Next, go to **Setup > System > Manage Global Variables** and check the Customized Variables tab for the Hotlink Type variable. If it has been customized, edit it and reset it to the default value of STANDARD.

You might also notice a setting in the People table called SSO Authentication Method. This field is set automatically by the system when you enable SSO, and should not be modified.