MemberFuse Single Sign On (SSO) API

MemberFuse provides an API allowing for the transfer of a user's session to and from enabled third party websites. The process is a One Pass Token (OPT) mechanism using a cookie passed to the user's browser when successfully logged in to MemberFuse.

Third party sites wishing to integrate SSO with MemberFuse need to do the following:

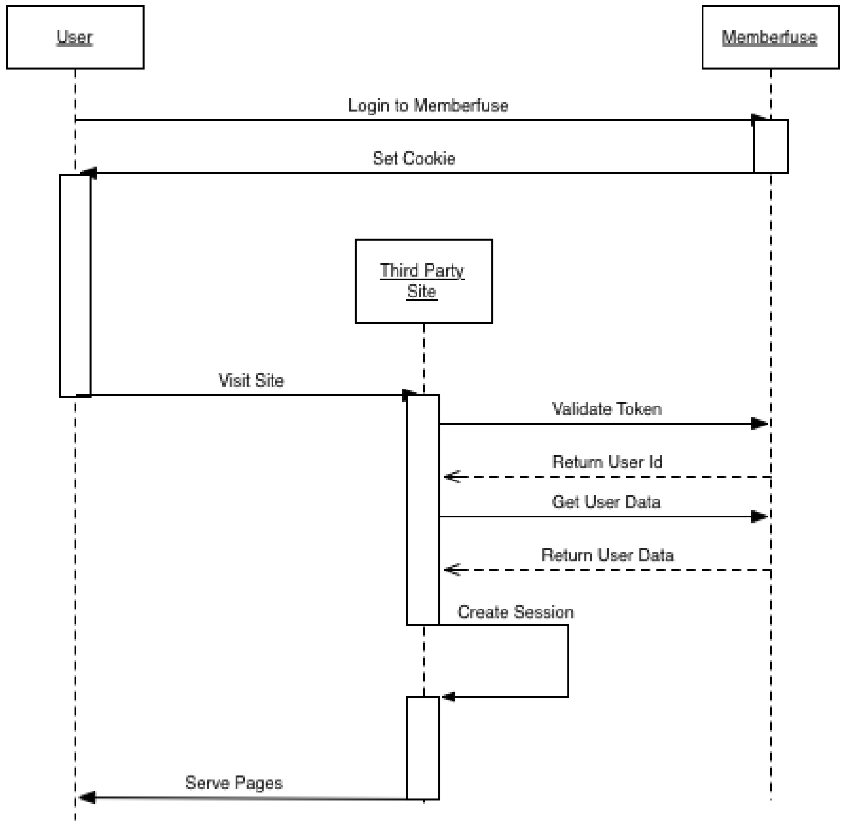
1. Ensure the third party site and the MemberFuse client site are running as sub-domains of the same root domain.

2. The third party site must be enabled in the MemberFuse client site to allow SSO from the third party.

SSO Authentication

The third party will need to modify its authentication scheme for a user. When a user visits a page you must check for the existence of a specific cookie. This cookie will contain a token identifying a logged in user in MemberFuse. Upon detection of the cookie the site will authenticate the token via a web service. If the token is valid, MemberFuse will return the ID of the user that the token represents. At this time, the third party site must create its session for the user indicated by the ID. If necessary, the site may also make a call to get the user's information (name, data, etc.). This is primarily for when the third party site does not store the user data itself.

If the third party site would like to allow a user to login from a page on their site, it will need to put an HTML login form on the page with markup supplied by MemberFuse. Details are listed below.



Web Services

All web services calls are made available via REST. They can be accessed using the URL http://www.siteurl.com/api , where www.siteurl.com is the URL of the MemberFuse installation.

All web service calls must be accompanied by an API KEY. The API KEY is a unique identifier issued by Avectra, and is only to be used by the application it was issued for.

validateToken

Checks to see if the input token is valid for the given api key and has a user with a valid session associated with it. A token can be found in the cookie located in the client browser, A token can only be validated once.

Input:

api_key:	**string – Supplied by Avectra**
token:	**string – Retrieved from user's cookie**

Output:

user_id:	**integer**

The function will return NULL on failure.

getUserData

Queries MemberFuse for user data for a user_id/site_id pair.

Input:

api_key:	**string – Supplied by Memberfuse**
user_id:	**integer**

Output:

user:	**User Object**

The function will return NULL on failure.

Cookie

On login into the MemberFuse Community a cookie is created for each integration domain. The cookie name for the specific application will be determined by Avectra. The contents of the cookie are simply a 'token' that can be used once with the validateToken() api call. This token is unique to the integration and user.

The existence of the cookie for an integration application is the confirmation to the application that the user has a current session with MemberFuse. Applications wishing to verify a current session needs only check the existence of a cookie.

On the initial session with the integration application user data can be fetched by using the validateToken() api call. The call will return NULL if the token has already been used, this however does not mean that the user is not logged into MemberFuse but simply that the token has already been passed into validateToken().

Login Form

The lack of a cookie means that the user is not logged into MemberFuse. In this case you should redirect a user to the MemberFuse login page with a redirect option to send them back to your application.

An example URL would be:

http://demo.MemberFuse.com/login?redirect=http%3A%2F%2Fwww.yoursite.com

Logout

Logout is a similar process to login. Using the MemberFuse logout page, will insure that the MemberFuse session is ended along with the integration application's session.

An example URL would be:

http://demo.MemberFuse.com/login/logout?redirect=http%3A%2F%2Fwww.yoursite.com

Cookie Alternative

Follow the process in MemberFuse to add a cookie using the Single Sign On Administration page. Enter the domain of your site and a name for the token. This token will only be accessible from the domain that you enter.

Once the token name and domain have been entered you may retrieve the token by making a request to the MemberFuse login page with a redirect variable that contains a url that will return to your site and a placeholder for the token.

Example:

http://demo.memberfuse.com/login?redirect=http://yoursite.com?token={token}

This will direct you to the MemberFuse login page. If the user is not logged in they will be prompted to login. If the user is already logged in, or after they completed the log in process, they will be redirected back to your site with the placeholder, "{token}", replaced with the token that is associated with the domain "yoursite.com". This token can be retrieved as many times as needed using the same method.

The validation of the token shares the same work flow as using the cookie method.