Recast

Liquit.SSO

Last Modified on 04.16.26

The *Liquit.SSO* function allows a user to connect to the Application Workspace API with previously authenticated credentials that are stored in the user's web browser. It also detects whether or not a user is already authenticated to an OAuth 2 provider configured in Application Workspace.
Within it, you can specify a username or identity source required to authenticate to Application Workspace and it can be either a Microsoft Entra ID (Azure AD) or an AD FS setup.
This can be useful in scenarios where multiple OAuth2 providers are configured and used by the user.

Request parameters

Name	Description	Default value
identitySource	This is the name of the identity source to authenticate the user with. Leave null for the default identity source.	null
username	The username for login. We recommend for the best experience to set this property as the actual name of the user because it can be used as a login hint or the user's mail address (UPN).	null
popUp	If true, the authentication process is started in a popup window.	false
token	The token used to authenticate the current user on the Application Workspace Server. For more information on how to set up your identity source to enable it to grant an exchange token, see How to set up your exchange token.	
callback	Invoked after someone tries to log in. If the login is successful, a token is generated. If the login is not successful, the response will contain an object called "fault" with a description of what caused the failure.	null

Example

```
Liquit.SSO({
  username: 'admin@recastsoftware.com',
  identitySource: 'Microsoft Entra ID',
  popUp: false,
  token:null //Exchange token
}, function(token, fault) {

  // Check if authentication failed.
  if (fault != null) {
    alert('Error ' + fault.code + ': ' + fault.message);
    return;
  }

  //Do Application Workspace stuff here

});
```