

Google SSO for Agiloft Contract Assistant

To configure OAuth SSO for your KB and the ACA, follow the steps in this article. This login works for both the ACA for Word and the ACA for Outlook, assuming that you have them connected to the same KBs.

In order to complete the configuration steps, you need a Google account, typically a Gmail address, to log in to the Google Developer Console. You may use any Google account to set up your Agiloft/OAuth project; it does not have to be associated with an Agiloft user. The address should be the one that you intend to use within Agiloft to sign on and access Google Docs.

Configuration

To configure OAuth SSO for your KB and the ACA, follow the steps below.

Step 1: Finding the KB Redirect Address

Before you can start setup in the Google Developer Console, you need to find the redirect address for the KB you want to set up. As the admin user, log in to the Agiloft KB where you want to set up OAuth/Google SSO.

1. Navigate to **Setup > Access > Configure OAuth 2.0 Profiles** and click New to create a new SSO profile.
2. Copy this text: `https://<server>:443/gui2/oauth20sso`
3. Click Cancel.

Step 2: Configuring the Google Developer Console

The following configuration steps are derived from the steps provided at <https://developers.google.com/accounts/docs/OAuth2Login#appsetup>. It is designed to help you integrate Google OAuth 2.0 SSO with Agiloft.

1. Log in to the [Google Developers Console](#) using the Google account.
2. Create a new project.
 - a. Click the drop-down at the top right and select Create a project.
 - b. In the next dialog box, enter a project name and click Create. You will then see the Project Dashboard.
3. In the Use Google APIs section, click Enable and manage APIs.
4. In the left pane of the API Manager window, click Credentials. If you wish to enable Google Docs integration with Agiloft, you can use the Drive API option in this window. This will be covered in more detail below.
 - a. In the Credentials dialog, select the OAuth consent screen tab.
 - i. Enter your Google Email address.
 - ii. Enter the Product name that will appear in the consent screen.

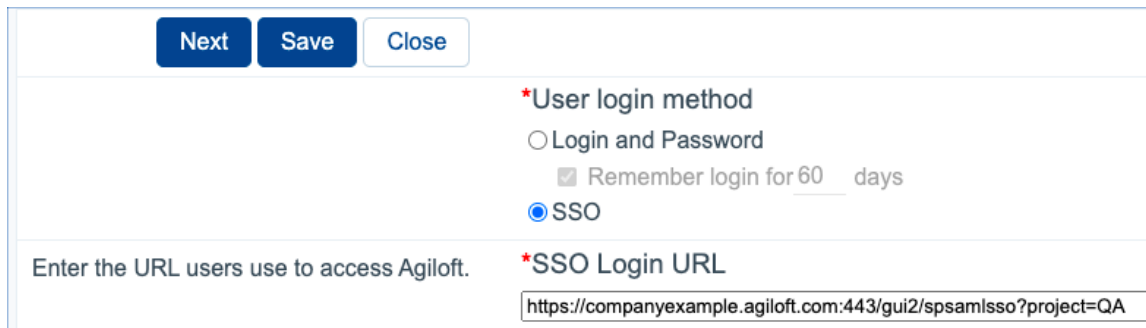
- iii. Optionally, enter the URL for the logo of your Agiloft instance, which will appear in the consent screen.
 - iv. Click Save.
- b. Select the Credentials tab, and select **Add credentials > OAuth 2.0 client ID**.
- c. Select the Web application radio button.
 - i. Optionally, enter a name for the web client.
 - ii. Leave the Authorized JavaScript origins field blank.
 - iii. In the Authorized redirect URIs field, enter the URL you copied from the KB.
 - iv. Save this URL, which will be used to create your OAuth profile in Agiloft.
 - v. Click Create.
- d. In the OAuth client dialog, save the client ID and client secret values. You will need to input the same values in the OAuth 2.0 Configuration wizard in each Agiloft KB where you will use Google OAuth 2.0 based SSO.

Step 3: Configuring SSO in the Agiloft KB

As the admin user, log in to the Agiloft KB where you want to set up OAuth/Google SSO.

1. Navigate to **Setup > Access > Configure OAuth 2.0 Profiles** and click New to create a new SSO profile.
2. Leave the Use full OAuth account name checkbox selected.
3. Enter a name for the OAuth 2.0 provider, such as Google.
4. For The role of the OAuth 2.0 Provider, select OAuth20_SSO.
5. Enter the following information in the remaining fields:
 - a. Redirect URI: Enter the value from step 1: `https://<server>:443/gui2/oauth20sso`
 - b. Client ID/Consumer Key: The client ID value provided above.
 - c. Client/Consumer Secret: The client secret value provided above.
 - d. Authentication URI: For Google OAuth 2.0 based SSO, enter `https://accounts.google.com/o/oauth2/auth`.
 - e. Token URI: For Google OAuth 2.0 based SSO, enter `https://accounts.google.com/o/oauth2/token`
 - f. Click Finish to save the OAuth 2.0 configuration.
6. To allow users to sign into Agiloft using Google OAuth 2.0 based SSO, ensure that at least one of the following conditions is satisfied:
 - a. The Login name of the Agiloft user is the same as the user's Gmail account.
 - or**
 - b. The Email Address of the Agiloft user is the same as the user's Gmail account.

7. In the ACA Configuration Wizard, make sure that the User login method is set to SSO, and include the URL from the setup page of the SSO configuration (The Redirect URI value). The SSO field should contain the https and include the entirety of the URL, like the example below:



The screenshot shows a configuration dialog box with three buttons at the top: 'Next' (dark blue), 'Save' (dark blue), and 'Close' (light blue). The main area is divided into two sections. The first section is titled '*User login method' and contains two radio button options: 'Login and Password' and 'SSO'. The 'SSO' option is selected. Below these options is a checkbox labeled 'Remember login for 60 days'. The second section is titled '*SSO Login URL' and contains a text input field with the URL 'https://companyexample.agiloft.com:443/gui2/spsamlso?project=QA'. To the left of this input field is the text 'Enter the URL users use to access Agiloft.'

8. Log out as the admin user.

Step 4: Signing In

Once the above steps are completed, Agiloft users will be able to log in to the ACA using their Google account. To sign in to the ACA:

1. Open the ACA and click Sign In.
2. Click Login via OAuth.
3. This brings you to the Google sign-on page. Simply input your credentials to continue to the ACA.
4. Once you log in successfully, the pop-up automatically closes and the add-in pane displays the main page.