Salesforce SAML Integration

Use this topic to assist you in configuring Agiloft with SAML using Salesforce as the Identity Provider. This way, you can establish a single sign-on connection between Salesforce and Agiloft, where Salesforce acts as the Identity Provider for SAML-based SSO. For more information on Salesforce configuration, see Salesforce Help. For more detailed information on configuring SAML in Agiloft, see SAML 2.0 SSO.

Prerequisites

To complete these steps, you need a Salesforce account with administrator access. You can sign up for a free trial account to use for testing. You also need admin access to your Agiloft Knowledgebase.

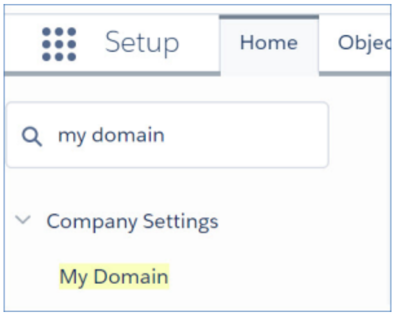
Register the Salesforce Domain

The full setup requires you to switch between Agiloft and Salesforce, so open each one in its own browser window so you can easily switch between them.

To begin:

1. In the Salesforce account, click the Setup icon to open the Setup Home.

   Note: You may need to switch to the new Salesforce Lightning interface at https://<domain name>.lightning.force.com/one/one.app#/home.
2. In the Quick Find search box in the left pane, enter "my domain", then select the search result.

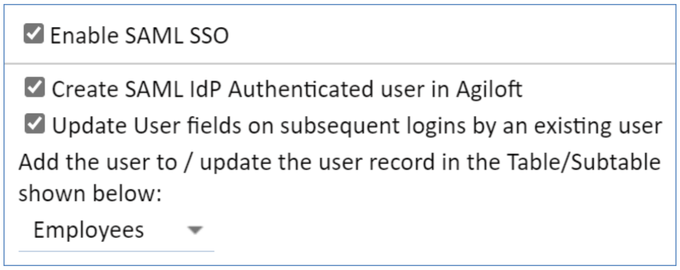
   my domain
3. Add a domain name in the field, and click Check Availability.
4. Once you find an available domain, click Register Domain
5. When the domain has been registered, you will receive an email to confirm that it is ready to use.

Configure Salesforce as an Identity Provider

1. In Salesforce Setup, enter "identity provider" in the Quick Find search box, then select the search result.
2. In the Identity Provider window, click Enable Identity Provider.
3. This opens the Identity Provider Setup window, which contains the necessary information to configure Agiloft.
4. Click Download Certificate and save the file to a location on your system.
5. Open the file in a text editor such as Notepad++ so that you can copy the contents.

Enable SAML in Agiloft

1. Click the **Setup** gear in the top-right corner and go to **Access > Configure SAML 2.0 Single Sign-On**.
2. In the General tab:
    a. Select Enable SAML SSO.
    b. Select Create SAML IdP Authenticated user in Agiloft, if you wish to provision a new user on login if one does not exist.
    c. Select Employees in the drop-down to add users to the Table/Subtable shown below.
    d. Select the last checkbox only if you want to synchronize the user attributes in Agiloft with those in Salesforce every time a user logs in. If you leave this deselected, the user's attributes will be synchronized only when the user is first created.



☑ Enable SAML SSO

☑ Create SAML IdP Authenticated user in Agiloft
☑ Update User fields on subsequent logins by an existing user
Add the user to / update the user record in the Table/Subtable shown below:
Employees ▾

General tab options

4. Select the Service Provider Details tab.
    a. For the Keystore file path, Java KeyStore Password, and Alias to add the certificate to the Java KeyStore...
        i. If you are using Agiloft's hosted service, the fields will be populated by Support.
        ii. If you are using an in-house server where Agiloft is installed, see Generate a Keystore File, and refer to the further information in the SAML 2.0 SSO topic to populate the fields.
5. Click Finish.
6. Download the Agiloft X.509 Certificate and and save it to your disk.
7. Click Configure SAML 2.0 Single Sign-On to reopen the SAML configuration wizard.
8. Leave the Service Provider Details tab open while you continue with the steps below.

Create a Connected App in Salesforce

1. In the Quick Find search box, enter "app manager", then select the search result.
2. In the Lightning Experience App manager window, click New Connected App.

3. Enter the app details in the Basic Information section based on your system.
4. In the Web App Settings, select Enable SAML. This will open additional fields which you must populate from the Agiloft Service Provider Details tab:
    a. Start URL - enter the base URL for the Agiloft knowledgebase. Whenever possible, make sure to use the domain name for your server, such as `example.agiloft.com`, rather than the specific server hostname, such as `ps108.agiloft.com`.
    b. Entity ID - enter the Agiloft (SP) Entity ID.
    c. ACS URL - enter the SAML V2 Assertion Consume Service (ACS) Endpoint.
    d. IdP Certificate - select the Default IdP Certificate. This will populate the Issuer and Name ID Format.
    e. Select Verify Request Signatures, then click Choose File to locate the Agiloft X.509 certificate from earlier.
    f. Click Save at the bottom.
5. In the Quick Find search box, enter "connected apps", then select the search result.
6. In the list of apps in the Connected Apps window, select the Master Label of the app you just created. This opens a view of the app details.
7. Click Download Metadata to download the app metadata XML file, and save it to a location on your system.
8. Open the metadata file in your text editor and copy the contents.
9. Click Manage Profiles.
10. Select the System Administrator profile, then click Save. This will give access to your current user profile which will enable you to test that the connection was established successfully.

Add Identity Provider Details in Agiloft

1. In the SAML Configuration wizard, select Identity Provider Details.
2. In "SAML Metadata XML contents obtained from your IdP", paste the contents of the Salesforce app metadata file.
3. Click Finish. This will automatically populate all of the Identity Provider Details fields, including the X.509 certificate, which is included in the metadata.

Establish the SAML Connection

1. To test the SAML connection from the IdP-initiated side, in the Salesforce window click the IdP Initiated Login URL. If the connection has been established successfully, this will open the Agiloft knowledgebase, with the user created.
2. To test the Agiloft-initiated login, point your browser to: `https://{server}/gui2/samlssologin.jsp?project={kbName}`, where {server} is the IP Address or FQDN of the server hosting the Agiloft instance and kbName is replaced by the name of your knowledgebase. Whenever possible, make sure to use the domain name for your server, such as `example.agiloft.com`, rather than the specific server hostname, such as `ps108.agiloft.com`.
    a. This URL forwards the login assertion to the IdP. You will be directed to the Salesforce SAML login page.
    b. If the user does not exist in the ADFS server, they will automatically be provisioned once ADFS authenticates the user successfully if you selected Create SAML IdP Authenticated user in Agiloft during the setup.
    c. If you are already logged in and authenticated, you will be forwarded directly to the Agiloft interface.

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.