


Ping Identity SAML Integration

This topic will assist you when configuring Agiloft with SAML using Ping Identity as the Identity Provider. For more information on Ping Identity configuration, see [Ping Identity Help](#). It will give you enough information to establish the single sign-on connection between Ping and Agiloft, where Ping acts as the Identity Provider for SAML-based SSO. For more detailed information on some of the steps in Agiloft, see [SAML 2.0 SSO](#).

Prerequisites

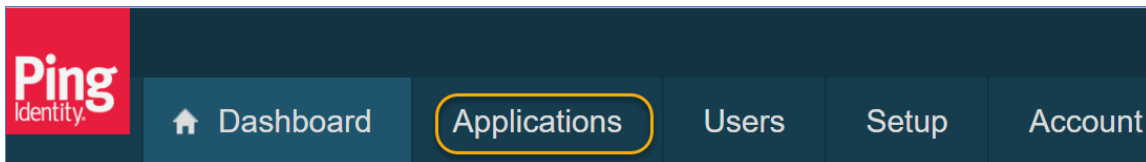
These steps require a Ping Identity account with administrator access. You can sign up for a [free trial account](#) to use for testing. You also need admin access to your Agiloft Knowledgebase.

Add a SAML Application in Ping

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

To add a SAML application in Ping:

1. Log into the Ping Admin Portal Dashboard, and select the Applications tab.



2. In the My Applications list, select **Add Application > New SAML Application**.
3. Add an Application Name, a Description, and upload a logo.
4. Click Continue to Next Step.
5. In the Application Configuration screen, with "I have the SAML configuration" selected, download the SAML Metadata to your disk.
6. Open the metadata file in a text editor such as Notepad++ and copy the contents.
7. Leave this window open while you configure the SAML wizard in Agiloft.

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.
 - 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 only be synchronized when the user is first created.

<input checked="" type="checkbox"/> Enable SAML SSO
<input checked="" type="checkbox"/> Create SAML IdP Authenticated user in Agiloft
<input checked="" type="checkbox"/> 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

3. 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.
4. Open the Identity Provider Details tab.
 - a. In the "SAML Metadata XML contents obtained from your IdP" field, paste the contents of the metadata XML file from Ping Identity. This will automatically populate the additional Identity Provider Details fields when the SAML wizard is reopened.
 - b. Click Finish.
5. Download the Agiloft X.509 Certificate and SAML 2.0 Service Provider Metadata files and save them to your disk.

Download X.509 Certificate
Download SAML 2.0 Service Provider Metadata

6. Click Configure SAML 2.0 Single Sign-On to reopen the SAML configuration wizard.
7. Leave the Service Provider Details tab open while you continue with the steps below.

Add Agiloft Details in Ping Identity

In Ping Identity:

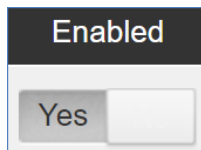
1. In the Ping Application setup window, ensure that the Protocol Version is SAML v 2.0.
2. Click Select File and locate the Agiloft XML file. When you upload the file, the Assertion Consumer Service (ACS) and Entity ID fields are populated automatically.

3. In Application 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`.
4. Next to Primary Verification Certificate, click Choose File and locate the Agiloft certificate.
5. Next to Signing, select Sign Response.
6. For the Signing Algorithm, select RSA_SHA256.
7. Click Continue to Next Step.
8. Click Save & Publish.

Test the Connection

In Ping Identity, test the connection:

1. To test the IdP-initiated login, in the Applications menu, select **Enabled > Yes** for the application you just created.



- a. Click the arrow to the right of the application.
 - b. Select the "Initiate Single Sign-On (SSO) URL"
 - c. Paste the URL into your browser. It will open an IdP initiated login to the knowledgebase, with your admin user as a newly created user.
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.
 - a. This URL forwards the login assertion to the IdP. You will be directed to the Ping Identity 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.