SAML 2.0 SSO

Agiloft integrates with a variety of SAML authentication providers, or Identity Providers (IdPs). SAML-based SSO is a leading method for providing federated access to multiple applications for your users or end users. This short guide assists you in configuring SAML authentication with your Agiloft knowledgebase.

SAML 2.0 Terminology

- **Identity Provider (IdP)** – Software that provides Authentication Service and uses SAML 2.0 protocol to assert valid users.
- **Service Provider (SP)** – Software that trusts an Identity Provider and consumes the services provided by the Identity Provider.
- **SAML Metadata XML** – An XML document containing SAML2.0 configuration data.
- **SAML Assertion XML** – An XML document that provides information about a user authenticated by an IdP.

Set Up SAML 2.0 SSO

The following highlights the steps needed to integrate any SAML 2.0 IdP with an Agiloft knowledgebase. Please refer to your IdP for instructions on how to configure access to a service provider, where Agiloft acts as the SP.

Prerequisites

To complete the setup, you need:

- Administrator-level login credentials for Agiloft and your SAML provider.
- Configuration details from your IdP. These are typically provided in an XML file, commonly known as IdP SAML Metadata XML. Download the XML file from your IdP. If your IdP does not provide the configuration via XML file, you must obtain the following details from the Identity Provider:
  - IdP Entity
  - IdP Login
  - IdP Logout URL
  - IdP X.509 certificate
- Optionally, the SAML Attribute names containing user groups and teams if you want to create users in Agiloft during login events. When you configure SAML SSO in Agiloft, you have the option to create users in Agiloft when they first log in. If you choose this option, you'll need to select which default groups and teams the user is assigned to, or map them from SAML attributes. You'll need the exact names of the SAML attributes containing the user's groups, teams, and Primary Team.

Configure Agiloft

Follow these steps in Agiloft to configure the SAML connection.

1. Log in to your Agiloft knowledgebase as an admin user.
2. Click the **Setup** gear in the top-right corner and click Access.
3. Click Configure SAML 2.0 Single Sign-on to open the SAML Configuration wizard.
4. On the General tab:
    a. Select the Enable SAML SSO checkbox.
    b. Optionally, select the "Create SAML IdP Authenticated user in Agiloft" checkbox. This creates users in Agiloft from those in the SAML system when the connection is first established. If this or the next option is selected, the User Field(s) Mapping tab appears when you click Next.
    c. Optionally, select "Update User fields on subsequent logins by an existing user." This updates the mapped user fields from SAML whenever the user logs in. If this option is selected, the User Field(s) Mapping tab appears.
    d. If the "Create SAML IdP Authenticated user" or "Update User fields on subsequent logins by an existing user" options were selected, choose a Persons table or subtable to map user fields from SAML to Agiloft.
5. User Group Mapping tab: Select any default Groups for the new SAML user, or map the user's group from an attribute in their SAML profile, at creation and on subsequent logins. You can set up user mapping after the initial configuration, too.
6. User Team Mapping tab: Select any default Team for the user, or use IdP or SAML attributes to define the team, at creation and on subsequent logins.
7. User Field(s) Mapping tab: If this tab is open, create the mappings between the SAML attributes and the field names of the Persons table in Agiloft. By default, this tab shows all of the field names of a user's record which can be mapped to SAML attributes. If you only want a specific set of field names to appear for mapping, you can restrict which fields appear using the List of fields from 'contact' table/subtable to be used in SAML configuration global variable.
8. The Service Provider Details tab contains information to connect to Agiloft as the Service Provider. Hosted customers must contact support to enter the provider details on this tab. Enter the following information:
    a. Agiloft (SP) Entity Id: Enter a unique identifier string for the Agiloft KB. Use the same identifier when configuring the Identify Provider. The system automatically populates this field with a value of `{server}/{KBName}`, e.g. `example.agiloft.com/mykb`. Replace any spaces in the Entity Id with the plus (+) symbol.
    b. SAML V2 Assertion Consumer Service (ACS) Endpoint: The value in this field should be in the form:

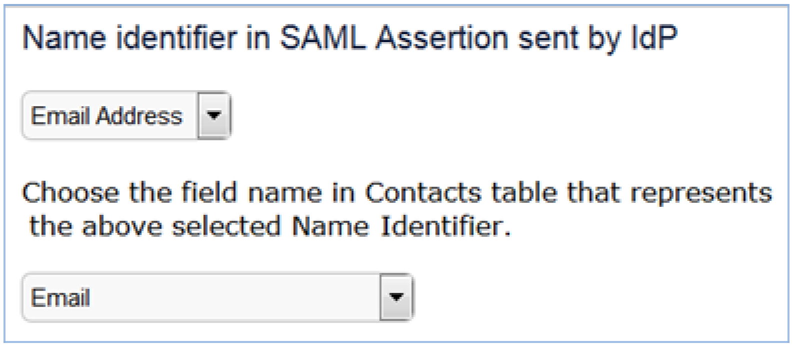
    ```
    http(s)://{server}/gui2/spsamlsso?project={KBName}
    ```

Write down these two values—they will be used to configure your Identity Provider (IdP). 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`.

c. Java Key Store (JKS) details. The Private Keys for HTTPS communication with Agiloft are stored in the Java Key Store (JKS) file on the Agiloft Server. The same Key pair will be used to digitally sign the SAML XML exchanged between the Agiloft server and IdP. For more assistance, see: Generate a Keystore File. Enter the following values:

   i. Java Keystore (.jks) file path on the Agiloft Server. Configurations vary by server. The default path for Agiloft servers is `/opt/server/Agiloft/etc/certs/agiloft.keystore`
   ii. Java KeyStore Password.
   iii. Alias used to add certificate to Java KeyStore.

d. Name identifier in SAML Assertion sent by IdP: In SAML 2.0 protocol, the NameID XML tag is used to send the details of the authenticated user in the SAML Assertion XML sent by an IdP to the service provider. From the drop-down, specify which format your IdP uses: User Name, Email, or Federation ID.



Name identifier in SAML Assertion sent by IdP

Email Address

Choose the field name in Contacts table that represents the above selected Name Identifier.

Email

Then, select the field name in the People table to match against the NameID value. If the NameID value in the XML assertion matches the value of the chosen field, then the user is allowed to log in to Agiloft.
Below is an example of a NameID TAG in SAML Assertion XML, which provides the email address of the authenticated user:

```
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:email"
>salesuser1@mydomain.com</saml:NameID>
```

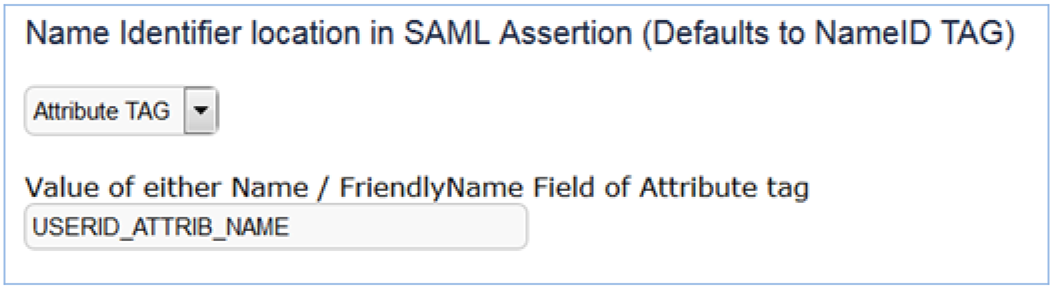
If your IdP sends a Federation Id for authenticated users, be sure to create a corresponding field in the People table and populate it with the correct value for the users accessing Agiloft via SAML.

e. Name Identifier location in SAML Assertion: Choose the XML tag - `NameID` or `Attribute -` used by the IdP to send user information. `NameID` is the most commonly used XML tag.
If your IdP sends user details in the Attribute TAG, enter the value of the `Name` or `FriendlyName` attribute. In the example below, `USERID_ATTRIB_NAME` is the value of the `Name` attribute:

```
<saml:Attribute FriendlyName="fooAttrib"
Name="USERID_ATTRIB_NAME"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">
salesuser1@mydomain.com

</saml:AttributeValue>     </saml:Attribute>
```



Name Identifier location in SAML Assertion (Defaults to NameID TAG)

Attribute TAG ▾

Value of either Name / FriendlyName Field of Attribute tag

USERID_ATTRIB_NAME

f. SAML Authentication Profile:

    - This option determines how Agiloft interacts with the IdP when a user tries to access Agiloft.
    - Select Passive Web Single Sign On with IdP to allow users who are already authenticated by the IdP to access Agiloft directly. If the user is not already authenticated, Agiloft shows an error message.
    - Select Forced Authentication to require a user name and password every time, even if the user has a valid login session with the IdP.
    - The Default behavior lets users who are already authenticated by the IdP to access Agiloft. If the user is not authenticated, the IdP prompts a login screen for the user.

g. Click Next.

9. On the Identity Provider Details tab:

    a. If you have a SAML Metadata XML file, paste the contents in the box under SAML Metadata XML contents obtained from your IdP. Leave remaining fields blank and click Next.

    When the SAML configuration is saved, Agiloft automatically populates the remaining fields based on the XML contents.

    b. Alternately, populate each field with the information previously obtained from the IdP. If you provide SAML Metadata XML in the first field and enter values in one or more of the remaining fields, the values entered in the individual fields override those obtained from the XML file.

        i. **IdP Entity ID / Issuer:** Enter the name or URL identifying the IdP.
        ii. **IdP Login URL:** Enter the URL where Agiloft should forward login requests.
        iii. **IdP Logout URL:** Enter the URL where Agiloft should forward logout assertions.

> ⚠ These logout assertions can be used for Single Logout (SLO), which is to say they can not only log a user out of their current Agiloft session, but out of all sessions for the browser that initiated the logout, requiring that the user then log into SSO again before beginning a new session with Agiloft or another SP. It may be necessary to leave this field blank in order to enable these logout assertions.

    iv. **IdP Provided X.509 Certificate Contents:** If your IdP provides the X.509 certificate in a file, open the file with a text editor and paste the contents of the certificate file in the input box.

10. Click Finish to save and close the SAML configuration wizard.
11. On the **Setup > Access** screen, click Download X.509 Certificate. Save this file to use when configuring the IdP.
12. On the **Setup > Access** screen, click Download SAML 2.0 Service Provider Metadata. Save this file to use when configuring the IdP. Note that this file also contains the X.509 Certificate, and most IdPs allow you to import this file to populate the fields in Configure the Identity Provider.
13. To enable SAML 2.0 for your users when they click a hyperlink sent within an email, change the Hotlink Type global variable to SAML20. You can do this on either the Admin Console or Power-User interface.
    a. Hyperlinks must use the Service Provider initiated SAML Login. An example of this URL is `https://test.agiloft.com/gui2/samlssologin.jsp?project=demokb&State=Edit:case&record=350&record_access=view&exiturl=leaveLoggedIn&cancelurl=leaveLogg`.
    b. The SAML Identity Provider should be configured to include the attribute InResponseTo, and the corresponding value, in the SAML assertion response that gets sent to Agiloft.

Note that SAML SSO Messages sent to Agiloft are encrypted using public key cryptography. Agiloft supports the following standard cipher transformations to prepare a message for encryption:

- RSA/ECB/PKCS1Padding
- RSA/ECB/OAEPWithSHA-1AndMGF1Padding
- RSA/ECB/OAEPWithSHA-256AndMGF1Padding
- RSA/ECB/OAEPWithSHA-512AndMGF1Padding

While these cipher transformations should suffice for most commonly used IdPs, if you find that your IdP uses a special cipher transform, you can configure Agiloft to use it with the Custom Cipher transform for decrypting SAML Keys global variable.

Generate a Keystore File

In cases where the Java Keystore file and corresponding private key are required for the SAML installation, which is typically needed when Agiloft is installed on a server which is not hosted by Agiloft, use the following steps to generate the Keystore file from the CA certificate and corresponding private key for your organization.

To configure Agiloft's SAML SSO Keystore file for servers hosted by Agiloft, please contact support.

Note that the OpenSSL tool is not present on Windows systems by default. You can download it here on the Agiloft server and use the same commands in Windows, after logging into the Windows server as an Administrator user.

1. Copy the CA certificate and private key files onto the Linux server where Agiloft is installed.
2. Login to the server via SSH.
3. Create a PKCS 12 file using your private key and CA signed certificate. The following OpenSSL command can be used to do this:

   ```
   openssl pkcs12 -export -in [path to CA certificate] -inkey [path to private
   key] -certfile [path to CA certificate ] -out mykeystore.p12
   ```

4. Create a JKS file using the Keytool command. Note that you may append the output file as either .jks or . keystore.

   ```
   <Agiloft_install_dir>/jre/bin/keytool -importkeystore -srckeystore mykeystore.
   p12 -srcstoretype pkcs12 -destkeystore mycompany.keystore    -deststoretype JKS
   ```

   a. When prompted, provide a new password for the destination keystore file: **mycompany.keystore**. Make a note of the password you use here.
   b. You may be prompted to provide an alias for the keystore. The default alias is 1.
5. Provide the complete path for **mycompany.keystore**, its password and the alias in the Service Provider Details tab of the Agiloft SAML configuration wizard.

Configure the Identity Provider

The next step is to provide the Agiloft Service Provider details to the IdP. Configuration steps for SAML 2.0 vary depending on the Identity Provider. Usually, you can import the SAML 2.0 Service Provider Metadata file to the IdP to populate these details, but below are the typical configuration items you are required to supply for the IdP:

1. Agiloft (SP) Entity Id, found in step 7.a. The default value is in the form:

```
{server}/{KBName}
```

2. Agiloft Login Assertion Consumer Service URL, found in step 7.b. The default value is in the form:

   ```
   http(s)://{server}/gui2/spsamlsso?project={KBName}
   ```

3. Agiloft Logout URL: This value is in the form:

   ```
   http(s)://{server}/gui2/samlv2Logout.jsp
   ```

4. Agiloft Logout Service End Point URL: This value is in the form:

   ```
   http(s)://{server}/gui2/spsamlssologout?project={KBName}
   ```

5. X.509 Certificate, downloaded previously.

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.

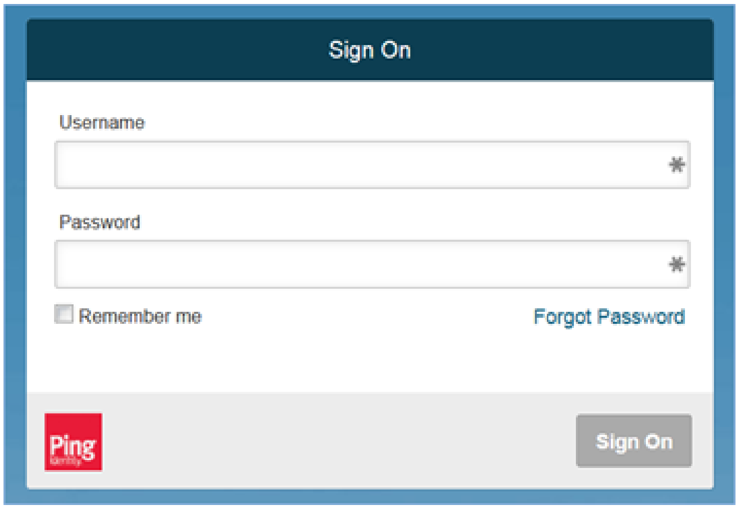
Next, go to **Setup > System > Manage Global Variables** and check the Customized Variables tab for the Hotlink Type variable. If it has been customized, edit it and reset it to the default value of STANDARD.

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.

Log In with SAML 2.0

Once the SAML 2.0 integration has been properly configured, users can log in to Agiloft by authenticating with the IdP.

1. Point your browser to: `http(s)://{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 Agiloft knowledgebase. 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`. Most users either save this URL as a bookmark (or favorite), or add an HTML login block to an existing web page.
2. This URL forwards the login assertion to the IdP and directs you to the login page for your IdP:



   If you are already logged in and authenticated, you are forwarded directly to the Agiloft interface.

Note: Agiloft supports SAMLv2 with Active Directory Federation Services (ADFS) version 2.0 and 3.0 in releases after 2015_02.