SAML 2.0

Single Sign-On Setup Guide

Last Updated: November 13, 2015

www.agiloft.com/documentation/saml-sso-setup.pdf

SAML 2.0 SSO SETUP GUIDE

This guide will assist you in configuring Agiloft to integrate with a Single Sign-On (SSO) identity provider using SAML 2.0 authentication. Single Sign-On with SAML 2.0 simplifies access for staff users and improves organizational security.

Introduction

Agiloft KnowledgeBases can be integrated with a SAML 2.0 *Identity Provider (IdP)* such as PingOne or Shibboleth. When using SAML 2.0 SSO, Agiloft acts as the *Service Provider (SP)***.** An application user authenticated by the *IdP* will be allowed to log in to Agiloft without further authentication by Agiloft.

SAML 2.0 Terminology

Identity Provider (IdP)	Software that provides Authentication Service and uses SAML 2.0 protocol assert valid users.
Service Provider (SP)	Software that trusts an Identity Provider and consumes the service provided by 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.

Setting 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, i.e. Agiloft.

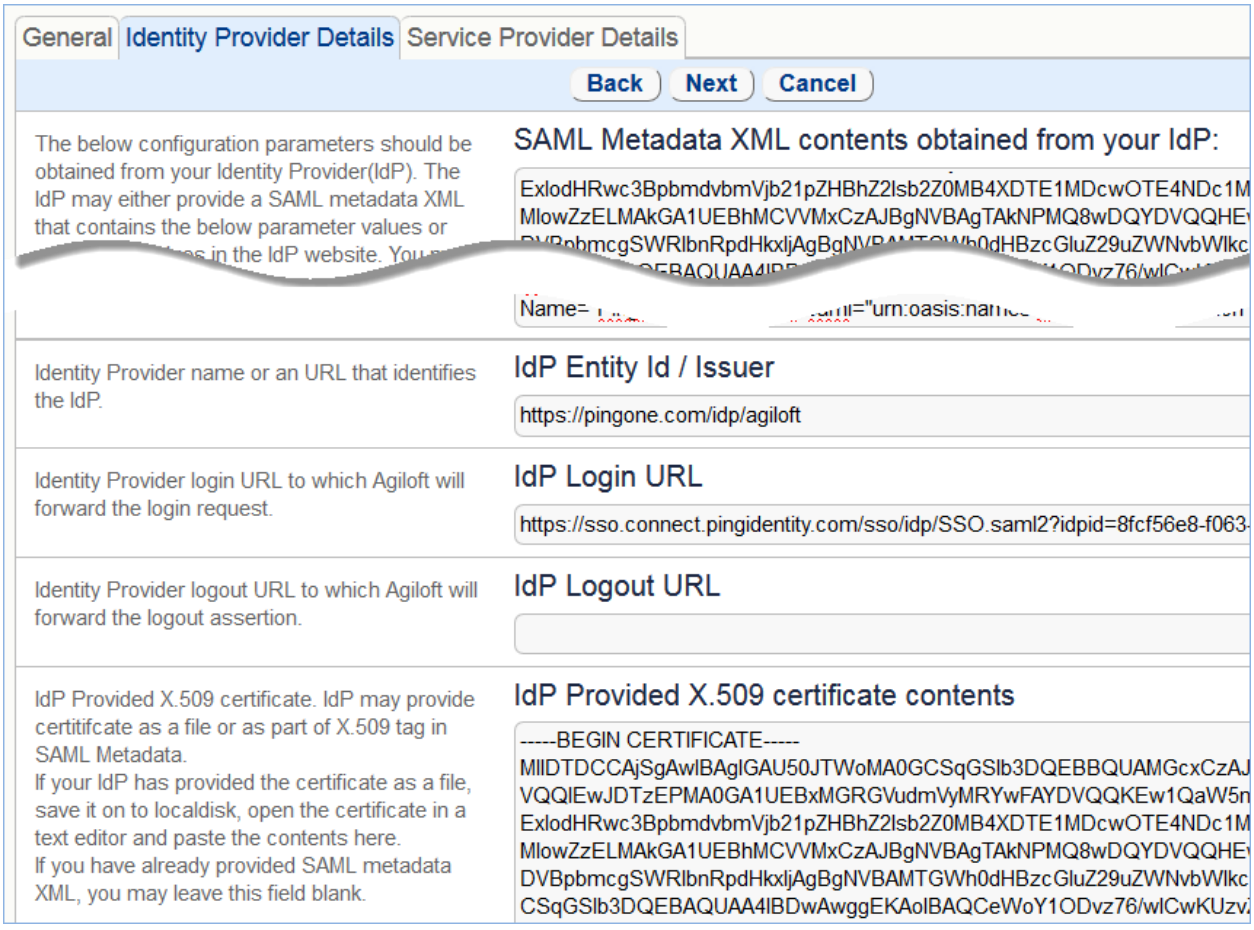
1. **Obtain configuration details from your IdP**:
    a. IdPs typically provide configuration details in an XML file, commonly known as *IdP SAML Metadata XML*. Download the XML file from you IdP.
    b. If your IdP does not provide the configuration via XML file, you must obtain the following details from the Identity Provider:
        i. IdP Entity Id
        ii. IdP Login URL
        iii. IdP Logout URL
        iv. IdP X.509 certificate
2. Log in to your Agiloft knowledgebase as an admin user and navigate to **Setup > Access**.
3. Click Configure SAML 2.0 Single Sign-on to open the SAML configuration wizard.

4. In the pop-up window, select the checkbox Enable SAML SSO and click Next.
5. 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.

> ***Note**: When the SAML configuration is saved, Agiloft will automatically populate the remaining fields based on the XML contents.*

    b. Alternately, populate each field with the information obtained in Step 1.b above.
        i. IdP Entity ID / Issuer: Enter the name or URL identifying the IdP.
        ii. IdP Login URL: Enter the URL where Agiloft will forward login requests.
        iii. IdP Logout URL: Enter the URL where Agiloft will forward 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.

> ***Note:** 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 will override those obtained from the XML file.*



6. Click Next.

7. On the Service Provider Details 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 will automatically populate this field with a value of `{server}/{KBName}`, e.g. `agiloft.example.com/mykb`.

   b. SAML V2 Assertion Consume Service (ACS) Endpoint: The system auto-populates this field with a value in the form:
   `http(s)://{server}/gui2/spsamlsso?project={KBName}`

> ***Note**: Write down these two values—they will be used to configure your IdP.*

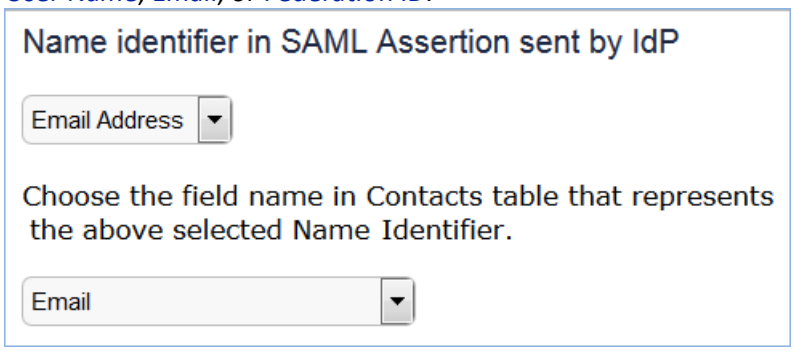
   c. **Java Key Store (JKS) details**. The Private Keys for HTTPS communication with Agiloft are stored in the Java Key Store (JKS) file on the Agiloft Server. The same Key pair will be used to digitally sign the SAML XML exchanged between the Agiloft server and IdP. Enter the following values:

      i. Java Keystore (.jks) file path on the Agiloft Server

      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.



   Then, select the field name in the People (contacts) table that will be matched against the NameID value. If the NameID value in the XML assertion matches the value of the chosen field, then the user will be 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:

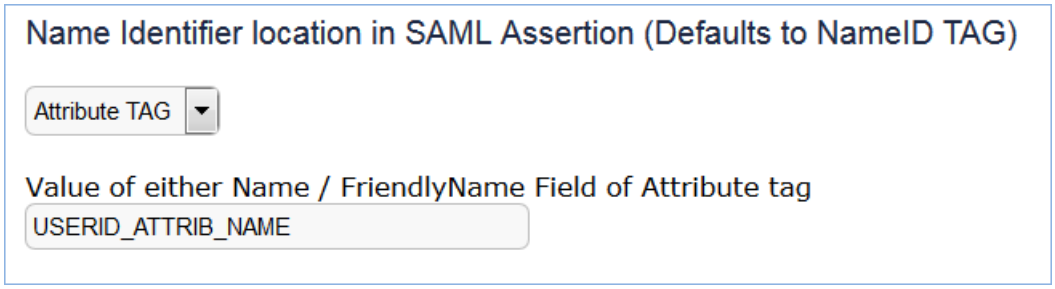
```
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:email">salesuser1@mydomain.com</saml:NameID>
```

> ***Note**: If your IdP sends a Federation Id for authenticated users, be sure to create a corresponding field in the People (contacts) 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>
```



f. SAML Authentication Profile: This option determines how Agiloft will interact 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 will display 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 will prompt a login screen for the user.

8. Click Finish to save and close the SAML configuration wizard.

9. On the **Setup > Access** screen, click Download X.509 Certificate. Save this file to use when configuring the IdP.

10. **Configure the Identity Provider with Agiloft Service Provider details**. Configuration steps for SAML 2.0 vary depending on the Identity Provider. You will typically need the following information from Agiloft (*Service Provider*) to configure an IdP:

    a. Agiloft (SP) Entity Id, found in step 7.a. The default value is in the form:
    `{server}/{KBName}`

    b. 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}`

    c. Agiloft Logout URL: This value is in the form:
    `http(s)://{server}/gui2/samlv2Logout.jsp`

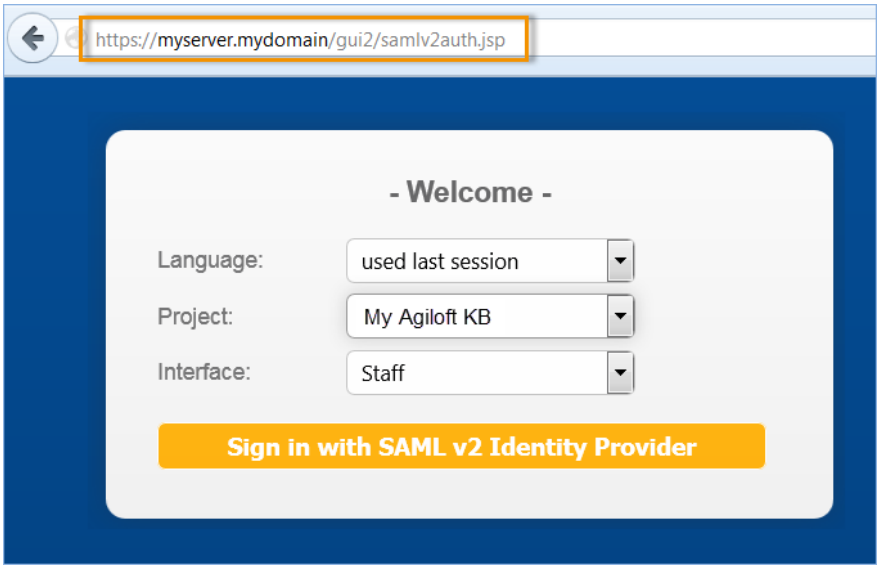
    d. Agiloft Logout Service End Point URL: This value is in the form:
    http(s)://{server}/gui2/spsamlssologout?project={KBName}

e. X.509 Certificate, downloaded in step 9.

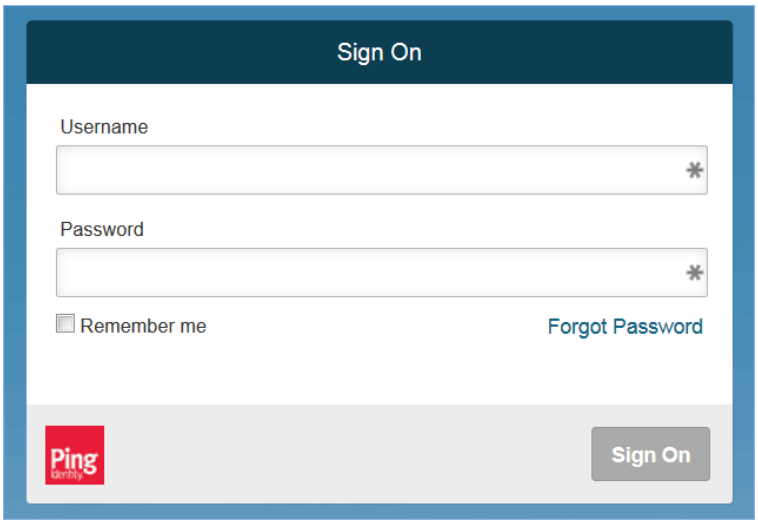
Logging in with SAML 2.0

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/samlv2auth.jsp` , where {server} is the IP Address or FQDN of the server hosting the Agiloft instance.



2. Click Sign in with SAML v2 Identity Provider. You will be directed to the IdP login page (in the screenshot below, PingOne is the Identity Provider):



Once successfully authenticated, the user will be taken to the Agiloft interface.