ADFS SAML Integration

This topic will enable you to set up Active Directory Federation Services (ADFS 2.0 and 3.0) with Agiloft SAML single sign-on. 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 also need to select which default groups and teams the user is assigned to, or map them from SAML attributes. You need the exact names of the SAML attributes containing the user's groups, teams, and Primary Team.

Prerequisites

- Administrator-level login credentials for Agiloft and the Windows server hosting ADFS.
- Obtain the configuration details from ADFS. These are typically provided in an XML file, commonly known as IdP SAML Metadata XML. Download the XML file from your ADFS server. Typically, for ADFS the IdP metadata can be downloaded from https://[ADFS SERVER]/FederationMetadata/2007-06/FederationMetadata.xml.
- If the ADFS server 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
- Note down the SAML Attribute names containing user groups and teams if you will create users in Agiloft during login events.

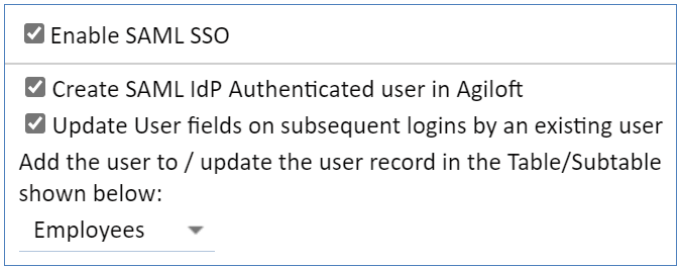
In Agiloft

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

The Agiloft-side instructions in this topic are focused on directions specific to ADFS. For detailed setup information, see SAML 2.0 SSO.

1. Navigate to **Setup > Access.**
2. Select Configure SAML 2.0 Single Sign-On.
3. On the General tab:
   a. Select Enable SAML SSO.
   b. Select Create SAML IdP Authenticated user in Agiloft, if auto-provisioning users is desired. If the option is not selected, only existing users of Agiloft can login via SAML SSO.

c. Select the last checkbox only if you want to synchronize the user attributes in Agiloft with those in the IdP every time a user logs in. If you leave this deselected, the user's attributes are synchronized once when the user is created, and then never synchronized again.



General tab options

d. Select Employees in the drop-down to add users to the Table/Subtable shown below.

4. Select the Service Provider Details tab.
5. Enter the Keystore file path, Java KeyStore Password, and Alias.
   Note: If you do not already have this information and you are a hosted customer, contact Agiloft support. If you are an on-premise customer, please see Generate a Keystore File.
6. On the Identity Provider Details tab, you need to enter the configuration details you should have obtained from the IdP as a Prerequisite. If you don't have the information yet, you can select the "Skip the validation" checkbox and click Finish to save your configuration as-is and return when you have the information. You need to enter:
   - SAML Metadata XML contents obtained from your IdP
   - IdP Entity ID/Issuer
   - IdP Login URL
   - IdP Logout URL
   - IdP Provided X.509 certificate contents
7. Click Finish.
8. Select Download SAML 2.0 Service Provider Metadata and save it where it is easily accessible. You will need to upload this file into the IdP in a later step.

In ADFS

Follow these steps to integrate ADFS 2.0 or 3.0:

1. In your Windows Server instance, open the ADFS Management Console.
2. Select the Relying Party Trusts folder and add a new Standard Relying Party Trust from the Actions sidebar.
   a. In the Select Data Source screen, select the second option and upload the Agiloft SP Metadata XML file.
   b. On the next screen, enter a Display name - for example, `SKS-Agiloft SAML`.
   c. On the next screen, select the ADFS profile radio button.

    d. On the next screen, choose whether to configure multi-factor authentication.
    e. On the next screen, select 'Permit all users to access this relying party.'
    f. On the next two screens, the wizard will display an overview of your settings.
    g. On the final screen click Close to exit and open the Claim Rules editor.
3. Once the relying party trust has been created, create the claim rules and update the Relying Party Trust (RPT) with minor changes that aren't set by the wizard. By default the Claim Rule editor opens once the trust has been created.
4. To create a new rule, click on Add Rule. Create a Send LDAP Attributes as Claims rule.
5. On the next screen, using Active Directory as your attribute store, do the following:
    a. In the LDAP Attribute column, select E-mail Addresses.
    b. In the Outgoing Claim Type, select E-mail Address.
    c. Click OK to save the new rule.
6. Create another new rule by clicking Add Rule, this time selecting Transform an Incoming Claim as the template.
7. On the next screen:
    a. Select E-mail Address as the Incoming Claim Type.
    b. For Outgoing Claim Type, select Name ID.
    c. For Outgoing Name ID Format, select Email.
    d. You need to modify the signing algorithm on your relying party trust. Select Properties from the Actions sidebar while you have the RPT selected.
    e. In the Advanced tab, switch from SHA-256 to SHA-1.
8. Once the relying party trust has been created, you can create the claim rules and update the RPT with minor changes that aren't set by the wizard. By default the claim rule editor opens once you created the trust.
9. Confirm the changes by clicking OK on the endpoint and the RPT properties.

Next, make a settings adjustment using PowerShell.

1. Run the ADFS PowerShell command: Set- ADFSRelyingPartyTrust -TargetName <Relying Party Trust Identifier> -SamlResponseSignature "MessageAndAssertion"
2. If you're using ADFS 3.0 or later, you're finished. If you aren't using ADFS 3.0 or later, use Remote Desktop (RDP) to access the AD system.
3. In the RDP, open PowerShell.
4. Add Windows PowerShell snap-ins to the current session.

At this point, ADFS is fully configured.

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 to Agiloft with ADFS

Once ADFS integration has been properly configured, users can log in to Agiloft by authenticating with the ADFS server.

1. 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`.
2. This URL forwards the login assertion to the IdP. You will be directed to the ADFS server login page.

3. 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.
4. If you are already logged in and authenticated, you will be forwarded directly to the Agiloft interface.