

Single Sign-On (SSO) for Authenticating Survey Respondents

SAML SSO authentication for survey respondents is available as an add-on. If you are interested in SSO, please [contact us](#) for additional information.

Are you already using an Identity Provider (IdP) to manage logins and access to the various systems your users need to access? If so, you can now include Alchemer as a Service Provider (SP) as part of your single sign-on (SSO). If you are not already using an IdP you probably won't start just for Alchemer.

We support any IdP that uses the SAML 2.0 protocol. At this time, we have tested SSO from Active Directory Federated Services (AD FS) and Azure (AD FS).

SSO Options in Alchemer

Within Alchemer you can use SSO to...

1. authenticate respondents into surveys. This tutorial will cover this option.

and/or

2. authenticate users into the Alchemer application to build and administer surveys. This option is covered in our [Single Sign-On \(SSO\) for Authenticating Alchemer Users Tutorial](#).

In both cases, SSO acts as an added security layer.

Why would I use SSO to authenticate survey respondents?

By authenticating your survey respondents via SSO you can lock your survey down so that only people who have IdP login credentials can access your survey. SSO authentication of survey respondents has an added benefit of leveraging any data present for each user in the IdP to prepopulate surveys. This data can then be used within the survey itself or in reporting.

What You Will Need Before You Get Started

If you're not an IT professional at your organization, go get one; you'll need his or her assistance to set this up.

Next, you'll need the below ingredients from your IdP; your IT professional can help you with this.

Entity ID - This is the globally-unique URL of your IdP entity. It's like a mailing address that we, the service provider, use to contact your IdP. Not sure where to find this? Learn more in

our [glossary of SSO terms](#).

Login URL - This is the URL/string for logging into your IdP. The Login URL is often very similar to the Entity ID URL. This is where we will send the SAML request.

SSL/Signing Certificate - We'll use your SSL certificate to encrypt the data being sent back and forth via SAML. You will need to upload your SSL Certificate from your IdP. Not sure where to find this? Learn more in our [glossary of SSO terms](#).

Alchemer-Side Set Up

You must be an account administrator in Alchemer in order to access these settings.

1. Go to **Account > Integrations > 3rd Party Integrations** and click the **Configure** button next to the **SSO Respondents** option.
2. Give your SSO Integration an **Internal Name**.
3. Choose the **Authentication type > Allow Respondents to take Surveys**. If you wish, you can select the option to **Force all new surveys to authenticate with this SSO**.

The screenshot shows the 'Single Sign-On' configuration page. At the top, there is a dark blue header with the text 'Single Sign-On'. Below this is a light blue informational box stating: 'uses the widely used SAML 2.0 protocol for single sign-on for Survey builders and Survey takers. Check this list to see if your provider is compatible.' The main configuration area includes three sections: 1. 'Integration Name' with a text input field containing 'SSO for Respondents'. 2. 'Authentication Type' with three radio button options: 'Allow Users to login to the [redacted] Application', 'Allow Respondents to take Surveys' (which is selected), and 'Force all new surveys to authenticate with this SSO'. 3. 'Status' with two radio button options: 'Enable SSO' (which is selected) and 'Disable SSO'. At the bottom of the form, there is a dark grey footer with the text 'Setup: Name Your SSO Integration and Select Authentication Type'.

4. Under **SAML Settings**, choose the **Name ID Policy** format that your IdP will provide to Alchemer in the SAML assertion. Your options are **unspecified** and **email**. Certain IdPs do not allow email addresses to be passed via the *unspecified* format.

SAML Settings

Name ID Policy

Pull SAML settings from Identity Provider Metadata
 Enter SAML settings manually

* Entity ID

* Login URL

Upload SSL/Signing Certificate
 No file chosen
 SSL Fingerprint:

5. Next, choose whether you wish to **Pull SAML settings from Identity Provider Metadata** or **Enter SAML settings manually**.
 - a. In order to use the option to **Pull SAML settings from Identity Provider Metadata** your metadata will need to be hosted somewhere so that you can provide a URL for our system to access and parse it.
 - i. Enter the URL to your hosted metadata xml file in the **Identity Provider Metadata URL** field.

SAML Settings

Pull SAML settings from Identity Provider Metadata
 Enter SAML settings manually

* Identity Provider Metadata URL

- b. If you prefer to enter your SAML settings manually, populate the **Entity ID**, **Login URL**, and **SSL/Signing Certificate** from your IdP. These fields are required.

SAML Settings

Name ID Policy

unspecified

Pull SAML settings from Identity Provider Metadata
 Enter SAML settings manually

Entity ID

https://samitest. .com/adfs/services/trust

Login URL

https://samitest. .com/adfs/ls/

Upload SSL/Signing Certificate

Choose File No file chosen

SSL Fingerprint: _____

Manual Setup Tips:

This is your **certificate file (.crt)** for your IdP which can be downloaded from your SSL Issuer.

- Files must include the the begin and end tags. The result should look like this:

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
```

- Files must be Base64 encoded.
- Use this [SSL Checker](#) to validate your file.
- If the file you have also has the 'intermediate' or 'root' certificate chains in them, that's fine, as long as it has the main certificate for the domain included.

- When you are finished with the SAML Settings, click **Save and Get Metadata**. The following **Service Provider Metadata** XML will be provided to you for you to use in the [IdP Setup](#).

Service Provider Metadata

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2017-02-
```

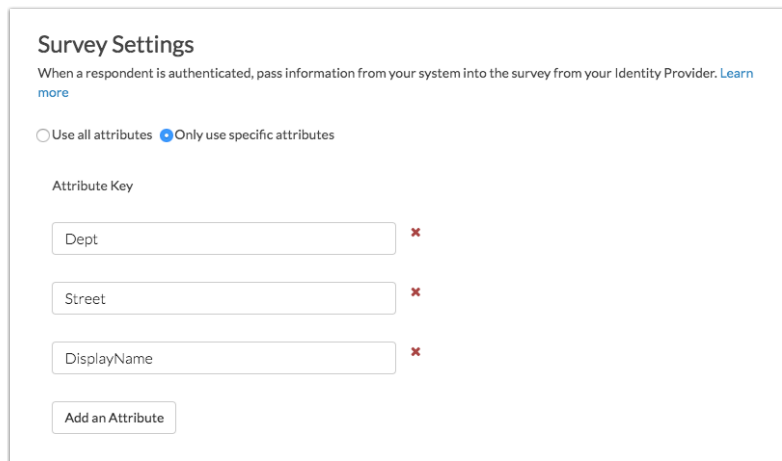
Integration Not Successful?

If the option to pull from metadata does not work we recommend trying the manual setup option. If you've tried both and neither were successful check out our [troubleshooting tips](#) for common causes of failure.

- Next, under **Survey Settings** you have the option to pass information from your IdP to your surveys.

If you wish to pass all information that your IdP is set up to send to Alchemer, select the option to **Use all attributes**.

If you wish to **only use specific attributes**, return to this step once you've completed your IdP setup. Once you've set up the attributes to send as described in the [step 8 of the IdP Setup Steps](#) section of this tutorial, you're ready to set up the data attributes from the IdP that you wish to store in Alchemer to use in surveys and reports. Click **Save** when you are finished adding all your attributes to be stored.



Now you're ready for the IdP-side setup!

IdP-Side Setup

Regardless of your specific IdP vendor, the setup on the IdP side requires:

- A claim rule with user's email address in Alchemer passed as the as the Name ID.
- (Optional) additional data from attributes can be sent to populate survey fields. [Learn more about populating survey fields.](#)

+ See [step-by-step example of the IdP-side setup with Active Directory \(AD FS\)](#)

Important Note Regarding Maintenance of Your SSO Integration

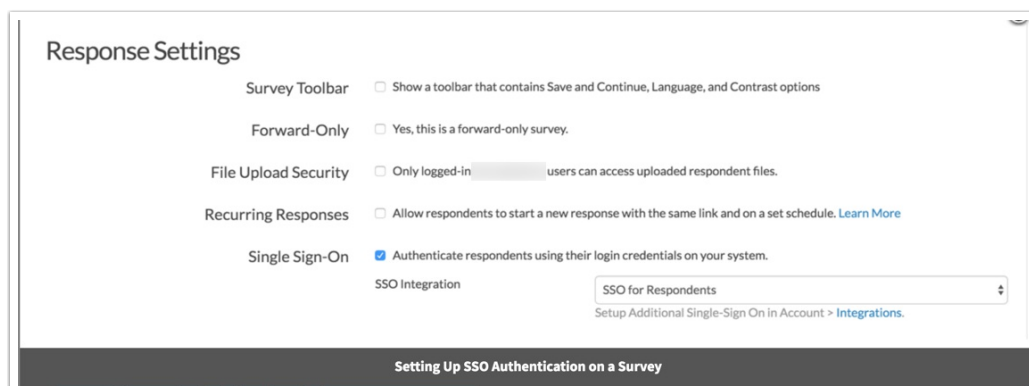
As we need to periodically update the cert used to create an SSL connection for SSO, we recommend putting a check in place so that your SSO integration is seamless. Once your integration is successfully set up, a simple script that checks for differences between the metadata in your integration setup and our SP metadata URL and accordingly handles updates to your integration ensures that there is no interruption in service.

Set Up SSO Authentication on a Survey

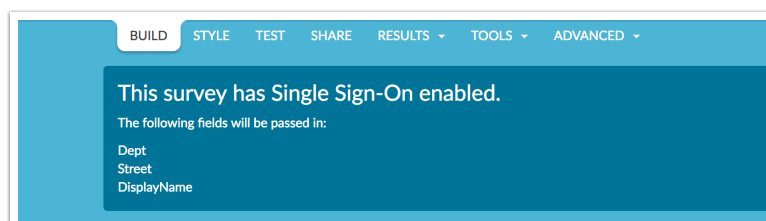
If you selected the option to **Force all new surveys to authenticate with this SSO** your surveys will be all set.

If you did not select this option, you'll need to manually set this up. To do so, go to **Tools > Response Settings** and check the option to **Authenticate respondents using their login**

credentials on your system. If you have more than one SSO integration set up for survey respondent authentication you'll need to select this in the dropdown menu. Click **Save Settings**.



When you return to the Build tab you will see the SSO data that are being passed into your survey.



Using SSO Data Attributes in your Survey

If you are passing in data attributes along with each survey respondent this data will be available by default for reporting purposes. But you might also want to reference this data in your survey. Using merge codes you can dynamically display and use data about each respondent to personalize the survey.

Using SSO Merge Codes to Customize Your Survey Text

Using merge codes you can create customized messages to personalize the survey experience.



In any text field throughout your survey, you will see the merge code helper available in the editor toolbar. Click this and scroll to the **Advanced** section and select **SSO Variable**.

MEDIA LOGIC LAYOUT PIPING / REPEAT

Text or Instructions

Greetings

What type of media?

- Text / Instructions
- Audio Player
- Video Player
- ReadyTalk Video
- Image

This will insert a default merge code. You'll need to replace the xxx with whatever your attribute name is as seen in your variable list at the top of the survey.

BUILD STYLE TEST SHARE RESULTS TOOLS ADVANCED

This survey has Single Sign-On enabled.

The following fields will be passed in:

- Dept
- Street
- DisplayName

When respondents access your survey this merge code will populate with the value in their user profile in your IdP.

SSO Survey

Greetings!

Greetings John Smith!

Thank you for taking the time to respond to the survey! This should take about 10 minutes.

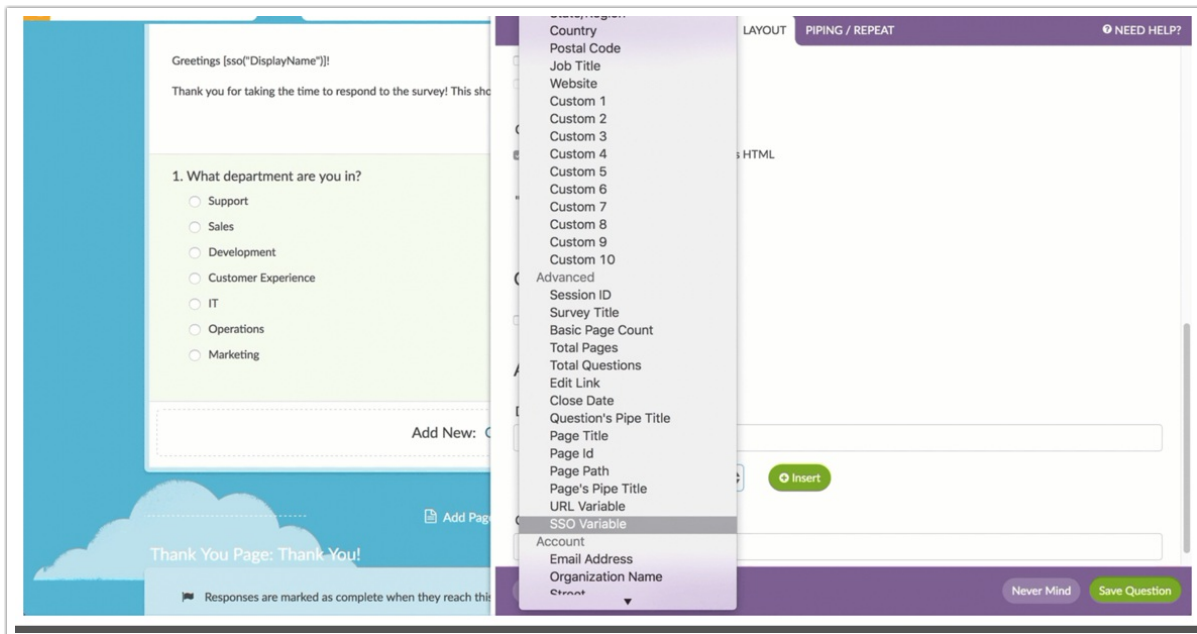
Using SSO Merge Codes to Pre-populate a Question

You can also pre-populate data you have in your IdP into questions.

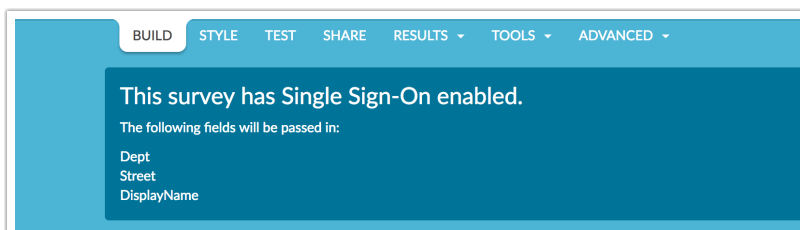
1. What department are you in?

- Support
- Sales
- Development
- Customer Experience
- IT
- Operations
- Marketing

To set this up edit your question and go to the **Layout** tab. Scroll to the **Default Answer** field and click the link to **Insert Merge Code**. Scroll to the **Advanced** section and select **SSO Variable**.



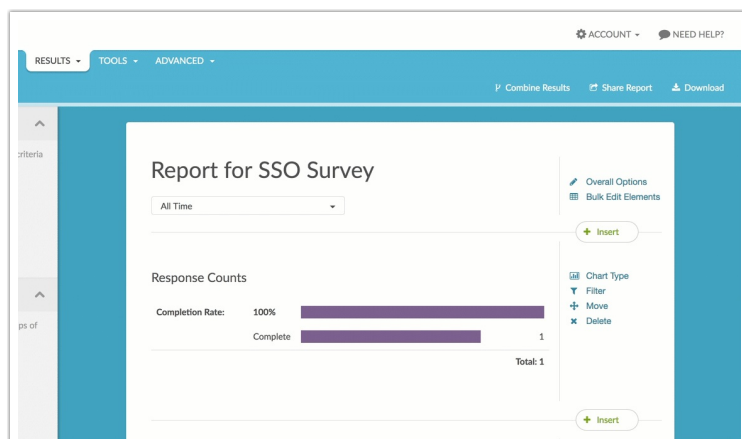
This will insert a default merge code. You'll need to replace the xxx with whatever your attribute name is as seen in your variable list at the top of the survey.



Reporting on SSO Data Attributes

You can report on your SSO data attributes in reports. To do so, click the **Insert** button and select **URL**, **SSO**, and **Hidden Values**. Then select your data attribute from the **SSO Attributes** section of the dropdown menu.

There are a number of [Chart Types available](#) for the SSO Attribute element.



Compatibility

This feature is not compatible with the following survey distribution methods:

- Offline Mode
- QR Code
- Kiosk Mode (online)
- Embedded Surveys

FAQ

- + How do I integrate with a sandbox environment?
- + What is the experience like for survey respondents?
- + How does SSO Authentication work with Email Campaign links? Save and Continue links? Edit links?
- + What happens if the survey respondent goes to the survey when they are not logged into the IdP?
- + Can I send survey data back to my IdP?
- + Can Alchemer supply a SAML Service Provider metadata file?
- + Can Alchemer's SAML consume the SAML IdP metadata file?
- + What attributes does Alchemer require within the SAML assertion?
- + Does Alchemer have a platform for testing identity federation?
- + Does your SP support SAML Single Logoff?
- + Does your SP support a logoff redirect following termination of the user session?
- + Does your SP sign the authentication (authn) requests that it sends to the SAML IDP?
- + Does your SP require a signature and/or encryption of the assertions issued by the SAML IDP?
- + Explain the user authorization mechanism employed by your SAAS application.
- + Can your SAAS application accept authorization (role membership) data from the SAML assertion?

Troubleshooting

- + I entered by entity ID, Login URL and uploaded my certificate, and my integration was not set up. What am I doing wrong?
- + If your Entity ID or Login URL are incorrect you will receive an error.

Glossary of SSO Terms

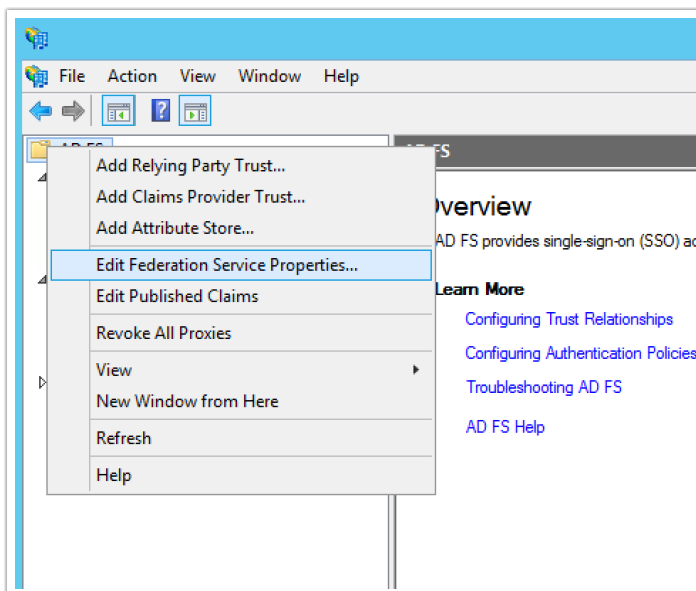
Active Directory Federated Services (AD FS)

Microsoft's IdP software.

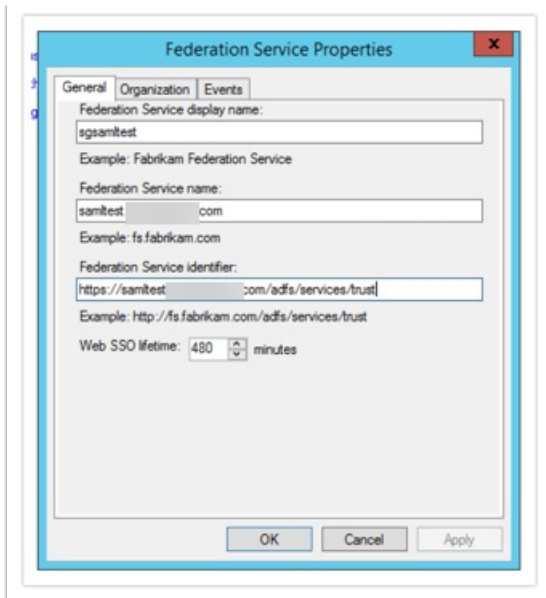
Entity ID

This is the globally unique URL/string of your IdP entity. It's like a mailing address that we, the service provider, use to contact your IdP.

Your Entity ID can be found in your AD FS Management Console by right-clicking the AD FS Folder and selecting **Edit Federation Service Properties**.



The URL in the **Federation Service identifier** field.



Identity Provider (IdP)

The source of truth for usernames and passwords.

Login URL

This is the URL for logging in to your IdP. The Login URL is often very similar to the Entity ID URL. This is where we will send the SAML request.

Name ID

Unique string to identify users. When sending Name ID to Alchemer we recommend it be their email address.

Service Provider (SP)

The web-based application/s that are accessed via the IdP.

Security Assertion Markup Language (SAML)

an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Single Sign-On (SSO)

Provides partner companies with full control over the authorization and authentication of hosted user accounts that can access web-based applications.

SSL Certificate

This is your certificate file (.crt) for your IdP which can be downloaded from your SSL Issuer. Files must be Base64 encoded. NOTE: If the file you have also has the 'intermediate' or 'root' certificate chains in them, that's fine, as long as it has the main certificate for the domain included.

User Principal Name (UPN)

The Name of the system user in email address format.
