Single Sign-On (SSO) for Authenticating SurveyGizmo Users

SAML SSO 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 SurveyGizmo as a Service Provider (SP) as part of this single sign-on (SSO).

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), Azure (AD FS), and Okta, Auth0, OneLogin, and Ping Identity.

SurveyGizmo has made improvements to our SAML 2.0 SSO integrations, to tighten security and provide greater ease of use in building out SSO integrations.

Please ensure you have the latest SP metadata before **September 10th, 2020** to prevent disruptions in your team's ability to login VIA your Identity Provider for previously created SSO integrations. You can use the automatically updating metadata URL found in each of your SSO integration setup pane(s) to ensure you always have up to date SP metadata certificates:

For more information view the Updating Service Provider Metadata Section of this documentation.

SSO Options in SurveyGizmo

Within SurveyGizmo you can use SSO to...

1. authenticate users into the SurveyGizmo application to build and administer surveys. This tutorial will cover this option.

and/or

2. authenticate respondents into surveys. This option is covered in our SSO Authentication for Survey Respondents Tutorial.

In both cases SSO acts as an added security layer. When using SSO for authenticating survey respondents there is also the added benefit of pre-population; any data present for each user in the IdP can be automatically passed into the survey, which can then be used within the survey itself or in reporting.

Why SAML SSO?

When security is of paramount importance, organizations will set up an Identity Provider (IdP) to manage all logins for all users. This allows IT professionals at the organization to control the number of logins out there in the wild. Identity providers also allow IT professionals to set up password reset rules to increase security.

If you are not already using an IdP you probably won't start just for SurveyGizmo.

How Does It Work?

Single sign-on allows organizations to set up a trust relationship with a service provider (SurveyGizmo in this case) that allows the IdP to send encrypted login credentials to the service provider thus preventing the user from having to log in more than once, hence single sign-on.

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.

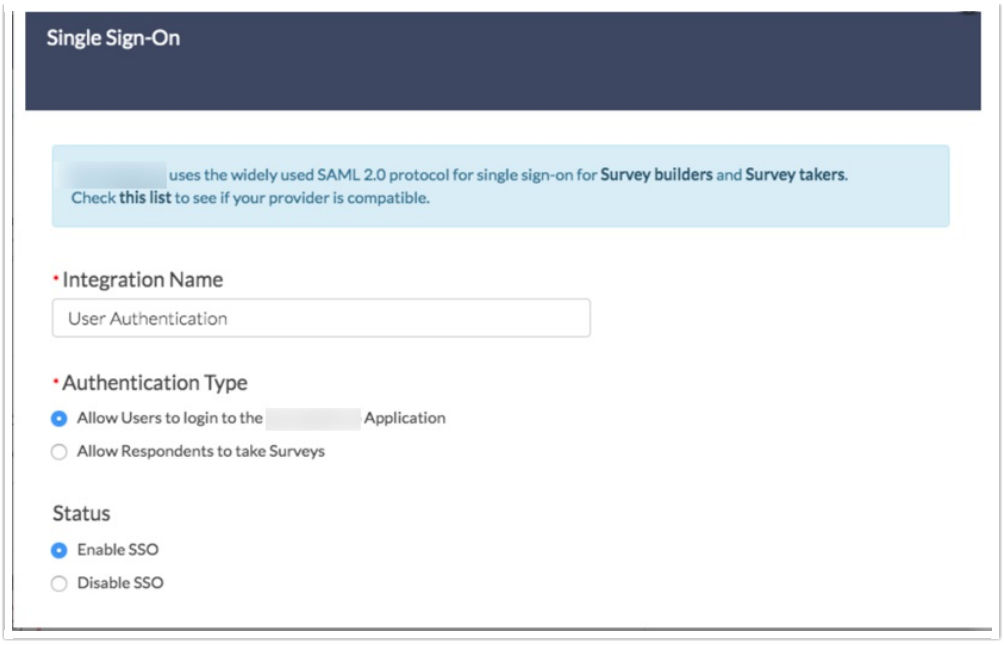
First, you'll need the below ingredients from your IdP; your IT professional can help you with this.

> **Entity ID** - This is the globally-unique URL/string 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.
>
> **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.
>
> **SSL/Signing Certificate** - We'll use your SSL/Signing 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.

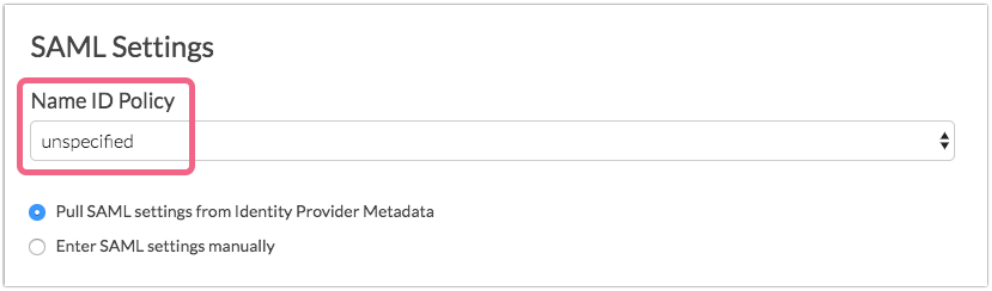
SurveyGizmo-Side Setup

You must be an administrative user in SurveyGizmo in order to access these settings.

1. From the Left Hand Navigation menu select **Integrations > Data Connectors** and click the Configure next to the SSO Users option under the *Enterprise Level integration* Section.
2. Give your SSO Integration an **Internal Name**. This is particularly important if you plan to use SSO both for authenticating users and for authenticating survey respondents as this name will display when setting up SSO authentication within surveys.
3. Choose the **Authentication type > Allow Users to log in to the SurveyGizmo Application** .



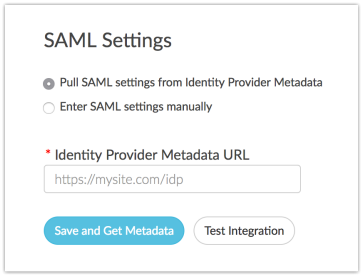
4. Under **SAML Settings**, choose the **Name ID Policy** format that your IdP will provide to SurveyGizmo in the SAML assertion. Your options are **unspecified** and **email**. Certain IdPs do not allow email addresses to be passed via the *unspecified* format.



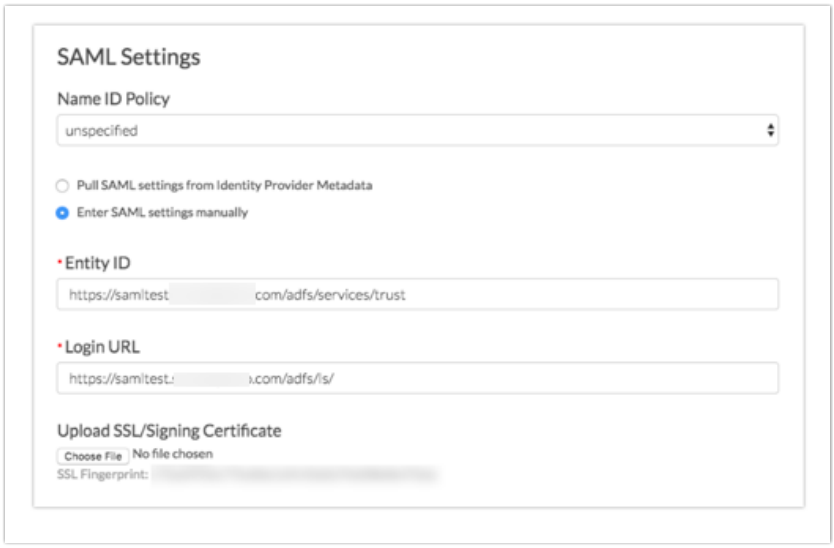
   a. Additionally there is **Signature Algorithm** dropdown, which relates to **Active Directory setups.** This can be left as SHA1 for most SSO builds. For Active Directory, select **SHA256:**
      i.

   b. Some iDP providers require **Signed Metadata.** Use this dropdown to navigate between **Yes and No:**
      i.

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



   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.



Manual Setup Tips:

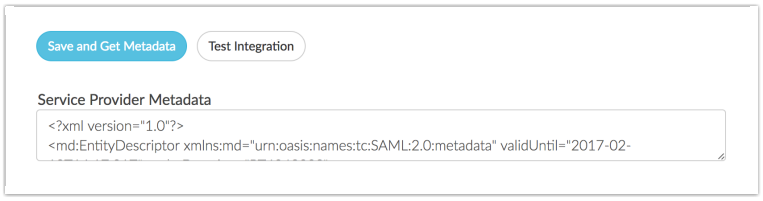
This is your **certificate file (.crt)** for your IdP which can be downloaded from your SSL Issuer.

- 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.

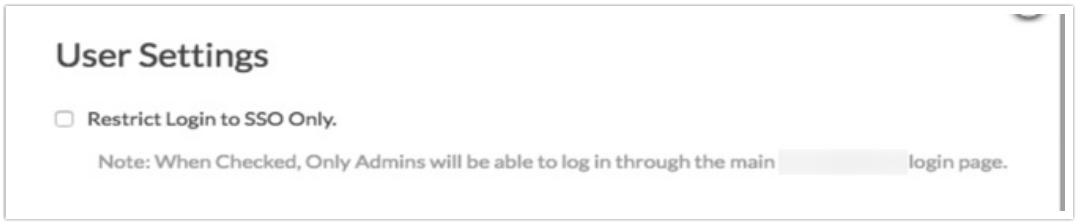
6. When you are finished with the SAML Settings click **Save and Get Metadata**. The following **Service Provider Metadata** XML will be provided to you for you to use in the IdP Setup.



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.

7. **(Optional) Restrict Login to SSO Only** - If you wish to *only allow users to access SurveyGizmo via your IdP*, check this box. If you wish to *allow users to login via either way*, IdP or SurveyGizmo, leave this unchecked.



The Restrict Login to SSO Only Setting will affect both who can access SurveyGizmo and how they will access SurveyGizmo.

- If the Restrict Login to SSO box is *unchecked* all users will be able to log in via both the IdP and SurveyGizmo, with the exception of users created via SSO.
- If the Restrict Login to SSO box is *checked*, any users that attempt to login directly via SurveyGizmo will not be able to and will see the following message:

  This account is restricted to Single Sign-On only. Please contact your account admin for assistance.

- Administrative users that were created in SurveyGizmo will always be able to log in via both the IdP and SurveyGizmo regardless of the status of the Restrict Login to SSO option.
- Users created via SSO will only be able to login via the IdP.

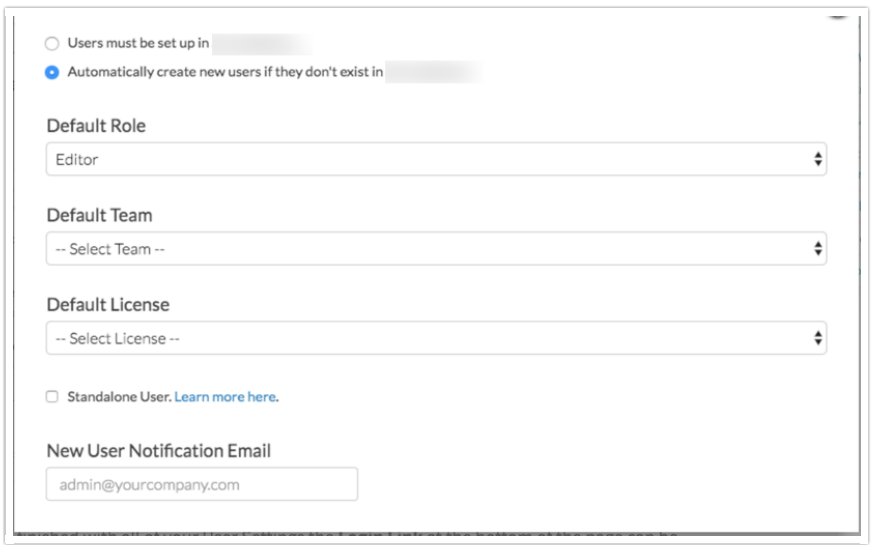
8. Next, there are two options that control how user seats in SurveyGizmo are handled:

   Users must be set up in SurveyGizmo - This means that administrative SurveyGizmo users will need to log in to SurveyGizmo via the SurveyGizmo log in page and add users as described in our Add Users Tutorial. Once a user is set up then the SSO via the IdP will work.

   OR

   Automatically create new users if they don't exist in SurveyGizmo - This option will create SurveyGizmo users when users click the link/button to log in to SurveyGizmo if a user with those credentials doesn't already exist in SurveyGizmo.

   - If you choose to automatically create new users, you'll need to specify a Default Role, Team, and License for these newly created users.
   - You will need to have enough licenses available in order to create the user. If there are no available licenses of the type you selected in the Default License field, the user will be created but disabled.
   - Check out our Teams and User Permissions Tutorial to learn more about Teams and Roles! Check out our User License Tutorial to learn about licenses.
   - As an alternative to selecting a default role and team, you can select the option to set up all SSO created users as Standalone Users. Standalone users will only be able to see the surveys that they create, regardless of team or role. Standalone users will have full access (meaning they will be Editors) to their own surveys (provided that their user license supports survey editing).
   - Finally, if you are automatically creating new users, it is a good idea to add an email address in the **New User Notification Email** field for the SurveyGizmo to send notification of user creation errors.



9. When you are finished with all of your User Settings the **Login Link** at the bottom of the page can be used to create a button within your IdP to log users into SurveyGizmo. This link will not work until you complete the IdP Setup below.

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 SurveyGizmo passed as the as the Name ID.
- (Optional) additional data from attributes can be sent to populate User Data Fields. Learn more about populating User Data Fields.

See a 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.

See a step-by-step example of the IdP-side setup with Okta

See a step-by-step example of the IdP-side setup of Auth0 SurveyGizmo SSO Integration

See a step-by-step example of the IdP-side setup of OneLogin SurveyGizmo SSO Integration

See a step-by-step example of the IdP-side setup of the Ping Identity SurveyGizmo SSO Integration

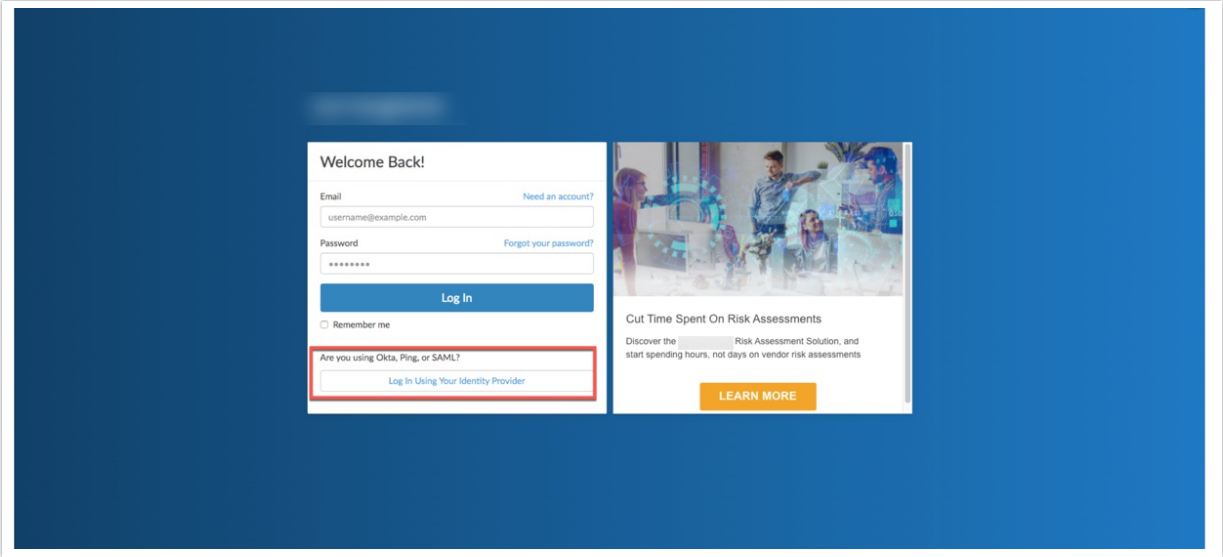
When logging into SurveyGizmo via the standard SurveyGizmo Login page (https://app.surveygizmo.com/login/) use the **default Email and Password** used when creating an account in SurveyGizmo.

Account Alias

An Account Alias is set up during or after a IDP integration has been created successfully via the provider of choice (Okta, Ping, etc.).

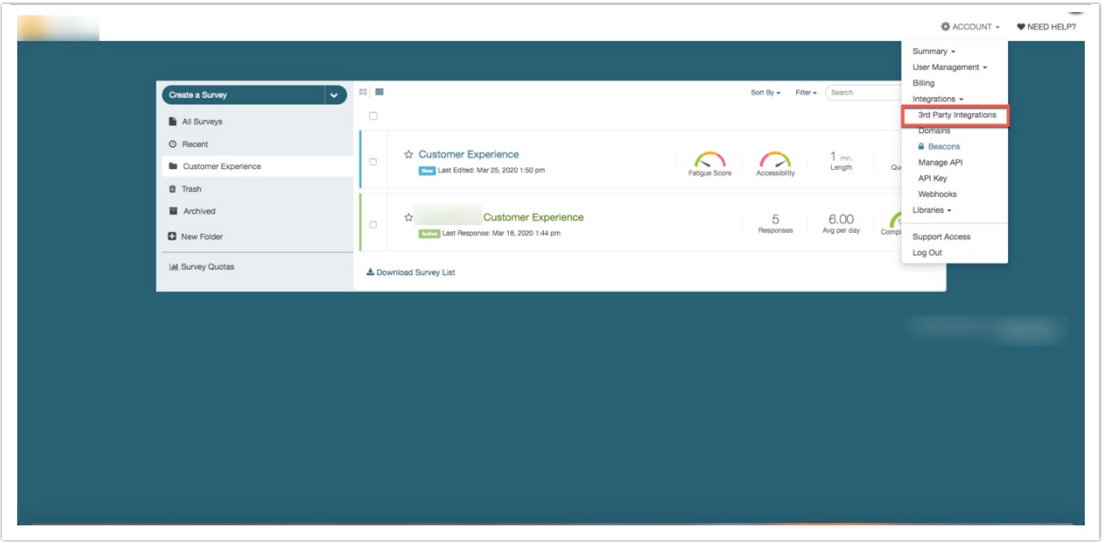
An Account Alias is utilized to identify a unique SSO connection within an application. Aliases allow a user who is set up with Single Sign-on in SurveyGizmo to login from SurveyGizmo through the identity provider that is being use. Simply, an Alias easily connects SurveyGizmo to an identity provider for a simpler login.

An Alias is set up within the **integration** for Single Sign-On for the SurveyGizmo account and is used on the SurveyGizmo Login page by selecting **Log In Using Your Identity Provider** at the bottom of the login window:

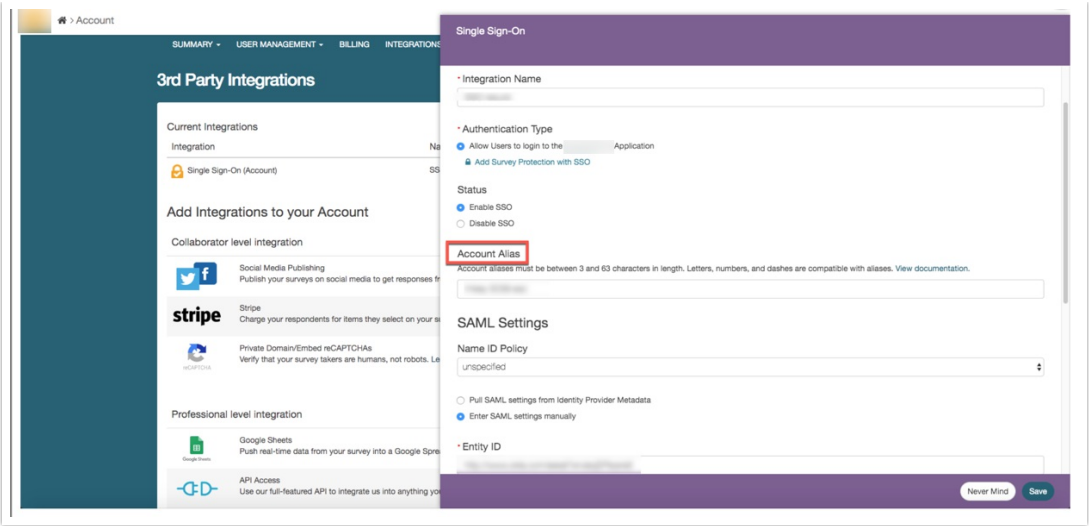


Setup

From the Left Hand Navigation menu, select **Integrations > Data Connectors.** Select **SSO Users** under the *Enterprise Level Integration* section:



Select **Edit** on the Single Sign-On integration to create an *Account Alias:*

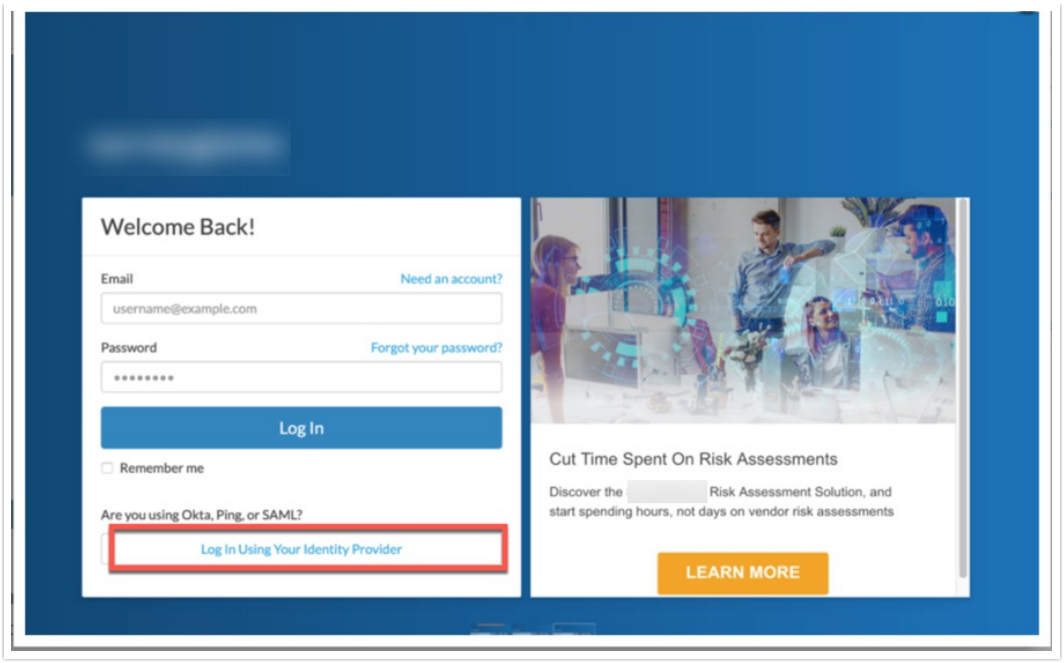


Provide a unique **Alias.** An Alias must be **between 3 and 63 characters** long and only **include letters, numbers, and dashes**. All other special characters are not compatible with Aliases in SurveyGizmo.

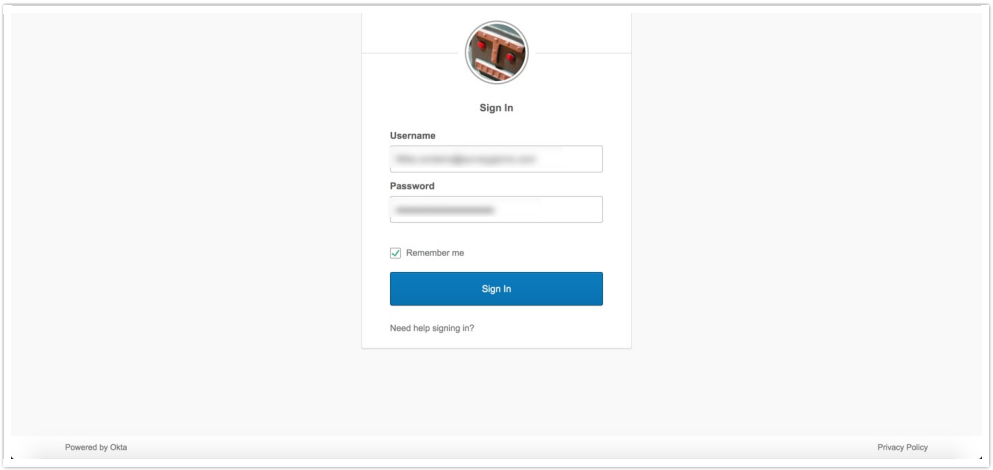
> Special considerations:
>
> - An Alias **cannot** start with a dash.
> - An Alias **cannot** end with dash.
> - An Alias **cannot** have multiple dashes in a row (--).
> - An Alias must be unique (no duplicate Aliases).
> - An Alias is not compatible across Data Centers (US, EU, CA).

Log In Using an Account Alias

Once an Account Alias is created on the dedicated IDP integration, navigate back to the login page. Select the **Login Using an Identity Provider** button, and provide the Alias that was created in the previous steps:



Click **Continue to your Identity Provider.** This redirects the user to the Identity Providers login page for authentication via the **Login Link** that exists in the integrations setup page:

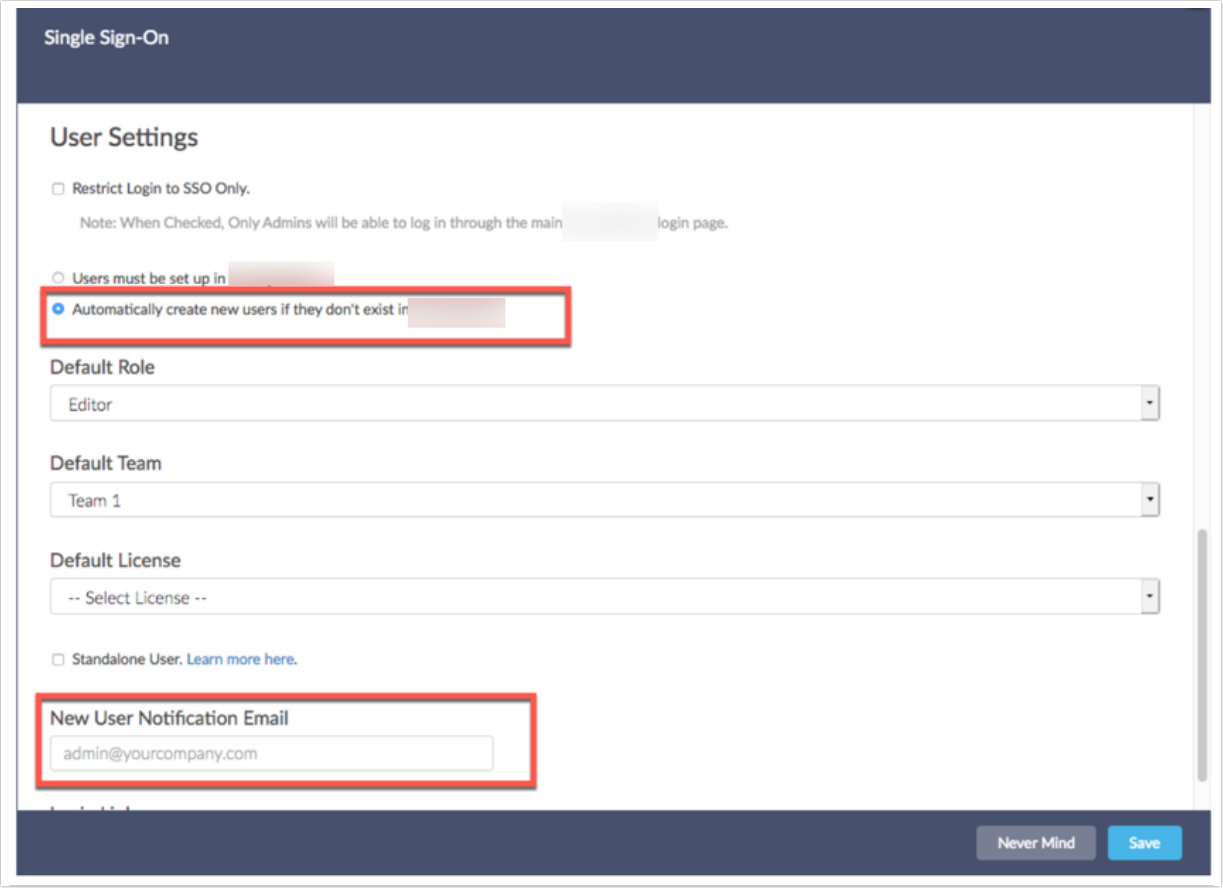


Users provide the login credentials associated with their identity provider via the unique link one is redirected to, and authenticated via the Identity provider before being redirected back SurveyGizmo. A cookie is stored in the browser for quicker login after the credentials for the IDP have been provided. Users see the Identity Providers login page load briefly before being brought to SurveyGizmo dashboard.

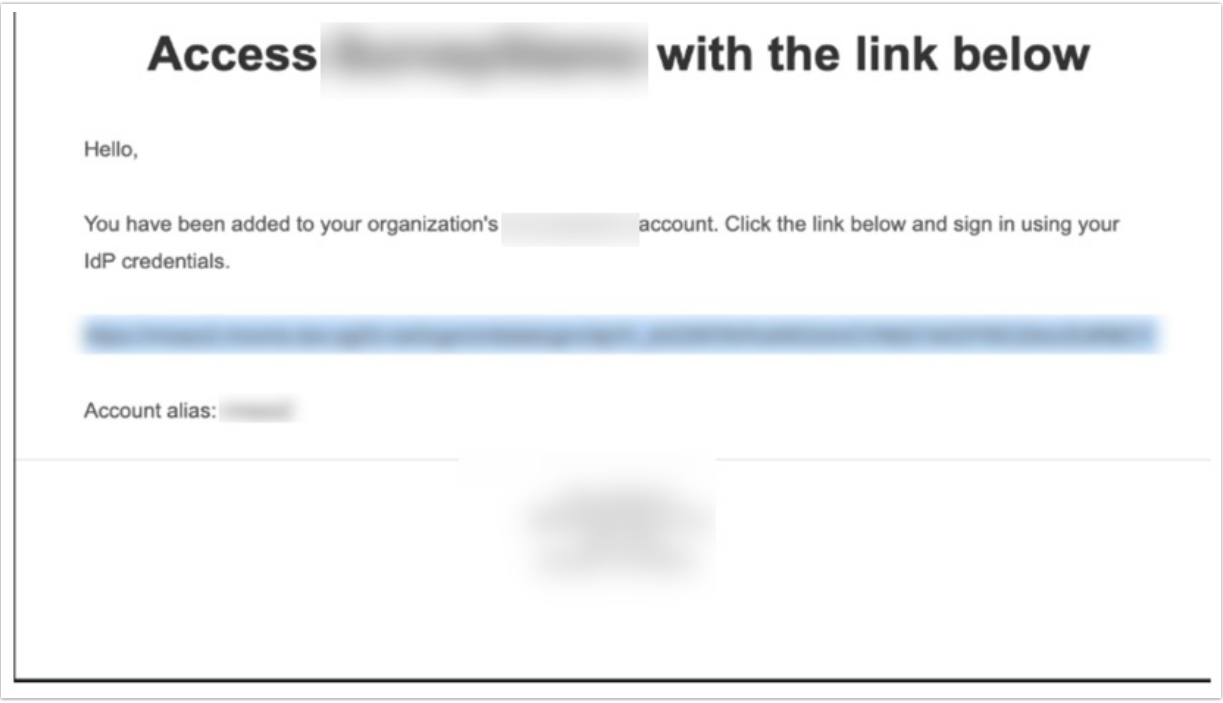
Creating New Users

Accounts utilizing the setting of **Restrict Login to SSO Only** forces users to access the account via the Identity Provider in use. When a new user is created in SurveyGizmo via Single Sign-On using the setting of **Automatically create new users if they don't exist in SurveyGizmo** , an email is triggered to the **New**

User Notification Email providing login credentials:



The email displays as seen below with the login link to access SurveyGizmo directly through the Identity provider as well as the Account Alias which is used on the main login page using the **Login using your Identity Provider** button:



Updating Service Provider Metadata

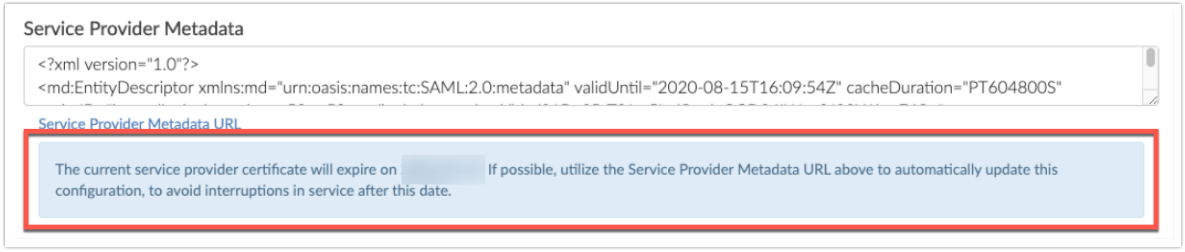
SurveyGizmo has made improvements to our SAML 2.0 integration! This is in efforts to tighten the overall security of the integration as well as provide an overall greater ease of use for Single Sign On. To ensure ease of access and proper functionality, most service providers will need the updated Metadata. It is highly recommended that users update their SP metadata prior to **September 10th, 2020** to make sure normal access is available for SSO and to avoid any interruption in services.

One can automatically update this information by clicking **save and get metadata** then selecting **Service Provider Metadata URL** found at the bottom of the Service Provider Metadata Text field to gain access to the most recent URL's and Certificates:

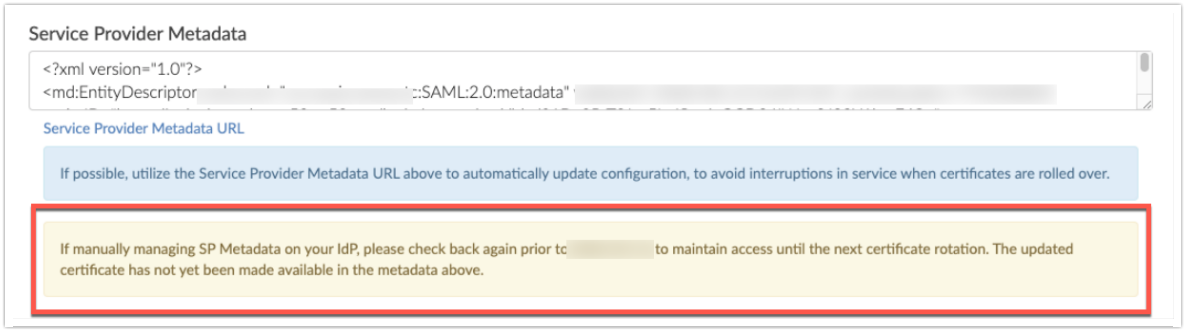
The Rollover certificate information is displayed within the **Service Provider Metadata box** as seen above!

Depending on the status of your certificate, one is displayed one of three banners to describe the status of the certificate that is in place. :

1. The blue banner displays when a functional certificate is in use on the integration after September 10th:
   a.

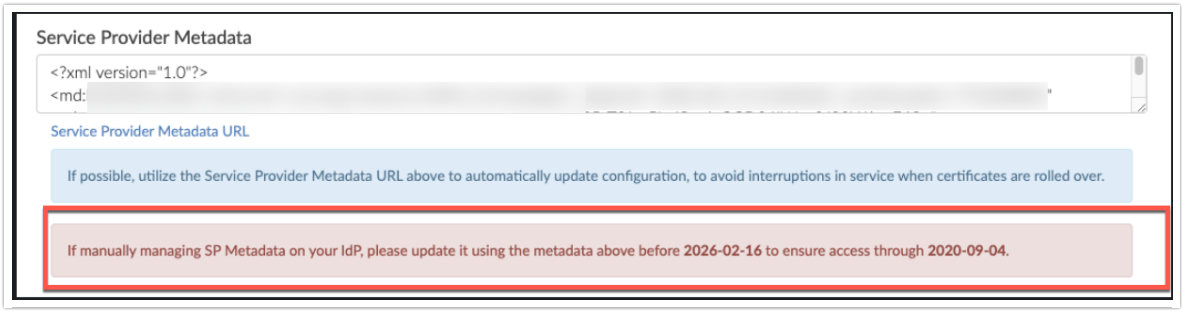


2. The Yellow banner is when there is less than 90 days to replace the certificate. This indicates users to come back and take action once SurveyGizmo rolls over the certificate:
   a.



3. The Red banner displays when a user needs to take action to update their metadata before SurveyGizmo rolls over the certificate by selecting the **Service Provider Metadata URL:**

a.



FAQ

- How do I integrate with a sandbox environment?
- What do I need to know to log existing SurveyGizmo users into that user via SSO?
- Okta is rejecting the Login link
- Will users still be able to log in with their login and password?
- Will my IdP login credentials work to log me into the SurveyGizmo login page?
- What happens if users try to log into the SurveyGizmo login page with IdP credentials?
- What happens if the IdP is unavailable? Typically you'll receive a browser message that the page cannot load.
- What happens when a SurveyGizmo session expires?
- Can I populate User Data Fields with SSO attributes?
- Can SurveyGizmo supply a SAML Service Provider metadata file?
- How do I deeplink to a specific page in SurveyGizmo?
- Can SurveyGizmo's SAML consume the SAML IdP metadata file?
- What attributes does SurveyGizmo require within the SAML assertion?
- Does SurveyGizmo 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?
- What happened to Automatic User Disabling?

Troubleshooting

- I entered by entity ID and 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)**
- **Entity ID**
- **Identity Provider (IdP)**
- **Login URL**
- **Name ID**
- **Service Provider (SP)**
- **Security Assertion Markup Language (SAML)**
- **Single Sign-On (SSO)**
- **SSL Certificate**
- **User Principal Name (UPN)**

Related Articles