

Using SAML with SSO

- [Overview](#)
 - [Signed Requests](#)
 - [Encrypted Requests](#)
- [Prepare for SAML implementation](#)
- [Setup SAML](#)
- [Enable SAML onboarding](#)
- [Customize data with CustomParameters and Parameters](#)
 - [SSO Entry Options](#)
 - [Custom Session Parameter Attribute](#)

Overview

Yellowfin 9.6 shipped with a new SAML interface to make secure connections simpler to set up and maintain for identity provider-initiated flows (such as Okta or Auth0). The new setup is slightly different to that of the old SAML bridge application, which is still available and functioning if you wish to implement additional features that the new, simplified interface does not provide (such as service provider-initiated flows).

SAML is an acronym for Security Assertion Markup Language. It's an XML-based open standard for the secure transfer of identity data between two entities — an identity provider (IdP) and a service provider (SP). The role of an identity provider is to authenticate and, if valid, pass a user's identity and authorization level to a service provider. The role of a service provider is to trust the identity provider and authorize a user's access to the requested resource.

Signed Requests

Yellowfin can manage signed requests from the identity provider to increase security. This feature is turned on by default, but requires some configuration. You must provide the signing certificate of the identity provider as well as the signing algorithm so that Yellowfin can decrypt the incoming signed requests. The identity provider should make these values obvious in their configuration.

Encrypted Requests

Yellowfin can also be configured to manage encrypted requests from the identity provider to further increase security. This can be toggled independently from the signed requests settings. You must generate an SSL key pair to give to Yellowfin (see `onelogin.saml2.sp.x509cert` and `onelogin.saml2.sp.privatekey` in the table on [this wiki page](#)). This is not provided by the system. Once you have those, you must then provide the private key and the certificate to Yellowfin in their respective configuration fields, as well as configure this setting in your identity provider and setup the SSL encryption certificate in their configuration.

Please note that this setting requires **PKCS#8 BEGIN PRIVATE KEY** format. If you have a different format, it will need to be converted.

[top](#)

Prepare for SAML implementation

Before setting up SAML within Yellowfin, make sure you have a good understanding of the fields you'll be required to address. The tables below provide further details for each of the fields.

Your IdP will require the following fields.

Parameter	Description	Required?	Default
Service Provider SSO URL	The Single Sign On endpoint URL that your IdP will use to reach the Yellowfin login page. This is typically your external base URL followed by <code>/SAMLLogin.i4</code>	Required	<code>ext_base_url /SAMLLogin.i4</code>
Audience Restriction	This is sometimes referred to as the 'Service Provider Entity Id' or 'Issuer Id'. It's the identifier of the Yellowfin SAML service. This is typically your external base URL followed by <code>/SAMLMetadata.i4</code>	Required	<code>ext_base_url /SAMLMetadata.i4</code>
Encryption Certificate	This certificate is used by the IdP to encrypt traffic going to Yellowfin. As mentioned earlier on this page, you must generate your own SSL key pair and provide the encryption certificate here.	Required if the toggle for Incoming Requests Encrypted is enabled	None

Yellowfin requires the following fields.

Parameter	Description	Required?	Default
-----------	-------------	-----------	---------

Identity Provider EntityId	<p>Sometimes referred to as the 'audience URI' or 'audience restriction', this identifies the entity of the service provider. This is typically in the format of</p> <p><your_idp_domain>/<sp_id></p> <p>For example,</p> <p>www.okta.com/ekti172b2ac0843Xf</p>	Required	None
Identity Provider SSO URL	<p>The Single Sign On endpoint URL of the SAML identity provider, which your IdP should display clearly within their own configuration page. This is in the format of:</p> <p><your_sso_domain>/<path_to_idp_sso_login></p> <p>For example,</p> <p>login.mybusiness.com/app/yellowfin1/ekti172b2ac0843Xf/sso</p>	Required	None
Identity Provider SLO URL	<p>The Single Logout endpoint URL of the SAML identity provider, which your IdP should display clearly within their own configuration page. This option tells Yellowfin where to point SLO responses. This is in the format of:</p> <p><your_slo_domain>/<path_to_idp_slo_logout></p> <p>For example,</p> <p>login.mybusiness.com/app/yellowfin1/ekti172b2ac0843Xf/slo</p>	Required	None
Identity Provider SLO URL Response	<p>This is an optional parameter which is only required if your IdP's endpoint for SLO responses is not the same as the one is uses for SLO requests. If nothing is entered, Yellowfin will use the URL entered in the Identity Provider SLO URL field. This is in the format of:</p> <p><your_slo_domain>/<path_to_idp_slo_logout_response></p> <p>For example,</p> <p>login.mybusiness.com/app/yellowfin1/ekti172b2ac0843Xf/sloresponse</p>	Optional	None
Identity Provider Certificate	<p>This certificate decrypts requests from the identity provider. Your identity provider should make this certificate obvious in their configuration.</p>	Required	None
Service Provider Private Key	<p>This private key decrypts incoming encrypted SAML requests from the identity provider. If you choose to enable this parameter, you must generate your own SSL key pair and provide the private key here.</p> <p>Although optional, we recommend that you provide this private key for Yellowfin to sign requests.</p>	Optional	None
Service Provider Certificate	<p>This certificate verifies the identity of the service provider and allows the identity provider to encrypt communications between services. If you choose to enable this parameter, you must generate your own SSL key pair and provide the encryption certificate here.</p> <p>Although optional, we recommend that you provide this private key for Yellowfin to sign requests.</p>	Optional	None
Signature Algorithm	<p>This algorithm verifies the incoming identity provider certificate. Choose from three different hash lengths to match whatever your incoming certificate uses:</p> <ul style="list-style-type: none"> • RSA-SHA256 • RSA-SHA384 • RSA-SHA512 <p>If you're not sure, use the default.</p>	Required	RSA-SHA256
Digest Algorithm	<p>This algorithm verifies the incoming identity provider certificate. Choose from three different hash lengths to match whatever your incoming certificate uses:</p> <ul style="list-style-type: none"> • SHA256 • SHA384 • SHA512 <p>If you're not sure, use the default.</p>	Required	SHA256
Incoming Requests Encrypted	<p>This toggle dictates whether incoming SAML requests will be encrypted by the identity provider. Switch on for higher security.</p>	Toggle	Off
UserId Attribute	<p>This field holds the Yellowfin user ID (typically a username or an email field, depending on your system configuration).</p>	Required	None
Client Reference Id Attribute	<p>This parameter provides the location of the Client Reference Id of the client org that the user belongs to. Normally, this is either left blank or set to '1' for Yellowfin instances that have no related client orgs.</p>	Not required	None
SSO Entry Options Attribute	<p>This parameter takes the SAML attribute that holds comma-separated web service session parameter values to be passed to the session created by the SAML SSO process. Leave blank to direct the user to their default entry page.</p> <p>See the Customize Data with CustomParameters and Parameters section for more details and an example.</p>	Not required	None


Custom Session Parameter Attribute	This parameter allows options that can be passed via the Parameters option on an SSO web service call to be passed to the session created by the SAML SSO process. This is attribute-based and can apply to individual users.	Not required	None
Onboard New Users	Enabling this toggle will allow SAML to provision new users automatically. If you don't wish to provision new users, do not enable the toggle.	Not required	Off

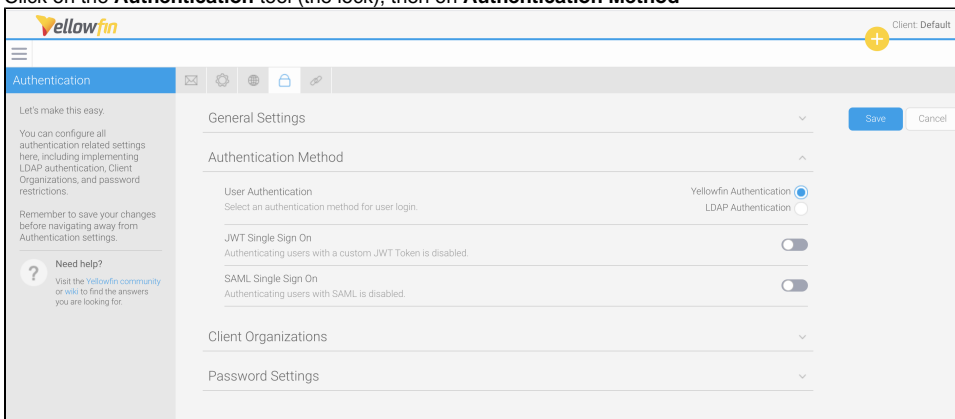
This page does not cover how to set up an identity provider, as there are many providers, each with different configuration processes. The page covers the basics that you will need to implement SAML for your Yellowfin users.

[top](#)

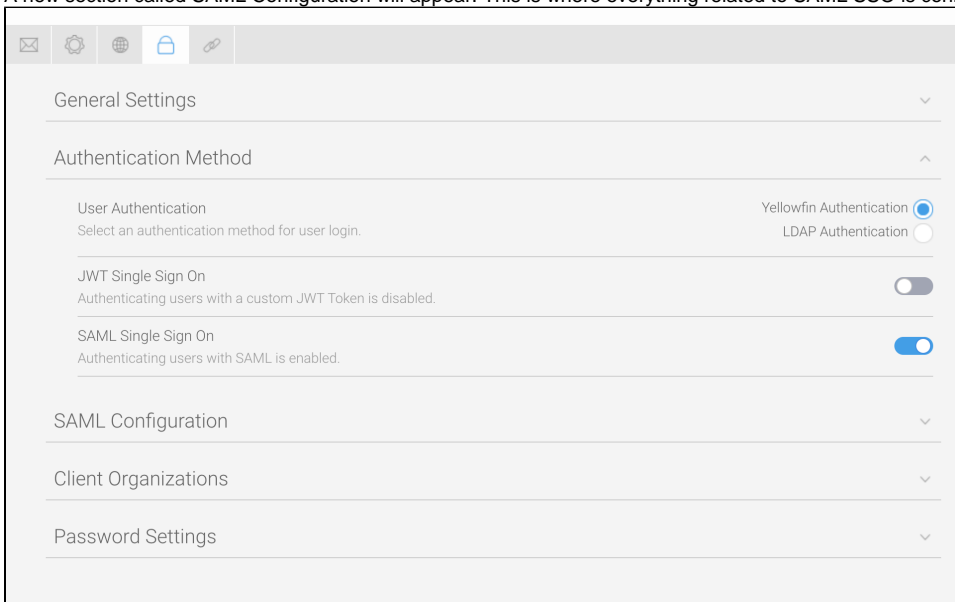
Setup SAML

To configure a SAML provider, follow the steps below.

1. From the Yellowfin burger bun menu  in the top left corner, click on **Administration**, then **Configuration**
2. Click on the **Authentication** tool (the lock), then on **Authentication Method**



3. Click on the toggle for **SAML Single Sign On** to enable it
A new section called **SAML Configuration** will appear. This is where everything related to SAML SSO is configured:



Click on **SAML Configuration** to expand the section

4. Refer to the preceding table to enter values for the required fields: **Identity Provider EntityId**, **Identity Provider SSO URL**, **Identity Provider SLO URL**, **Identity Provider Certificate**, **Signature Algorithm**, **Digest Algorithm**, and **User Id Attribute**

5. Refer to the preceding table and the following content to enter any other values for the other, non-mandatory fields described (see the image below for an example)

SAML Configuration

Identity Provider EntityId

Enter the EntityId of the SAML identity provider.

www.myip.com/ekti172b2ac0843Xf

Identity Provider SSO URL

Enter the SSO endpoint URL of the SAML identity provider.

login.mybusiness.com/app/yellowfin1/e

Identity Provider SLO URL

Enter the SLO endpoint URL of the SAML identity provider.

login.mybusiness.com/app/yellowfin1/e

Identity Provider SLO Response URL

Enter the SLO response endpoint URL of the SAML identity provider. Depending on your IdP, this may be optional, since some providers require a different response endpoint. If not specified, the SLO endpoint is used.

Identity Provider Certificate

Enter the certificate of the identity provider. This certificate will decrypt requests from the identity provider.

E1lbGlxITaFbGNVBaOMGEIudGVybmv0IFdpZGdpdHMgUHR5IEx0ZDENMAsGA1UECwwEZHNhZjAeFw0xNzAyMDEwNTQyMDIafw0yNzAyMDEwNTQyMDIafMFWxZCZAJBgNVBAYTAkFtYmVwQWwCgYDVQIDANWamWxMDALBgNVBACMBE1lbGlxITaFbGNVBaOMGEIudGVybmv0IFdpZGdpdHMgUHR5IEx0ZDENMAsGA1UECwwEZHNhZjCCASiwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPWlwy8Wcm/tm4V0G8BB9ALM8/BuXXNm837pIAKceCVmQlgtNaA2DD6vehm3zLH+ovLoHHvU/0b1uNHxmHZ/Gf2bc5IJNXxwEAjQO/eGbgbsD9fziSJWWIvVMKmvMEU3iOpY71h4xflZsMcK8CEbPtVSAJcJQf

Service Provider Private Key

Enter the private key that will be used to sign, encrypt and decrypt SAML messages between the application and the IdP.

m837pIAKce1lbGlxITaFbGNVBaO1uNhMGEIudGVybmv0IFdpZGdpdHMgUHR5IEx0ZDENMAsGA1UECwwEZHNhZjAeFw0xNzAyMDEwNTQyMDIafMFWxZCZAJBgNVBAYTAkFtYmVwQWwCgYDVQIDANWamWxMDALBgNVBACMBE1lbGlxITaFbGNVBaOMGEIudGVybmv0IFdpZGdpdHMgUHR5IEx0ZDENMAsGA1UECwwEZHNhZjCCASiwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPWlwy8Wcm/tm4V0G8BB9ALM8/BuXXNm837pIAKceCVmQlgtNaA2DD6vehm3zLH+ovLoHHvU/0b1uNHxmHZ/Gf2bc5IJNXxwEAjQO/eGbgbsD9fziSJWWIvVMKmvMEU3iOpY71h4xflZsMcK8CEbPtVSAJcJQf

Service Provider Certificate

Enter the certificate that will be used to sign, encrypt and decrypt messages between the application and the IdP.

NKnaCfsrYIPirHh6C5HTYj4LnKroal1yrHdeKy97q4XpNXqej7H81UDpoFPY2pu3HrgNVX4T0upNXuDGZFWypp2GJb11CCEof9juowum0ENcnb3Vvk3FmINHrFh7F9PgefC3HrGWo+HCGGvNZfppn5K3qew2GZfpGdyfvsy1vWS9TyEws9Q86CdT8ODqWypQLGJPWoRpbRzq2pw6iCdFeCVYm489yJEINvjv59iFTSTKEd8FZuillJlFmINv6u5CUiUfJucTxssXpNXfUAYEvFswrRiKCA/JHBUzQU4pdJNN5OCB3bWsrC5+re1054Tou+DiYBYABxrTQAgph09KA2nP1X/Dlafw0yNzAyMDEwNTQyMD

Signature Algorithm

Select the algorithm used when signing outgoing SAML messages

RSA-SHA256

RSA-SHA384

RSA-SHA512

Digest Algorithm

Select the digest algorithm used when signing outgoing SAML messages

SHA256

SHA384

SHA512

Incoming Requests Encrypted

Incoming SAML requests will be encrypted by the identity provider for improved security.

UserId Attribute

Enter the SAML attribute name that holds the User Id login value.

yf_user

Client Reference Id Attribute

Enter the SAML attribute name that holds the Client Reference Id login value.

SSO Entry Options Attribute

Enter the SAML attribute that holds the value of comma-separated webservice session parameters to pass to the session created by SAML SSO. Leave blank if there are no session parameters to pass.

Custom Session Parameter Attribute

Enter the SAML attribute that holds the value of a custom variable to pass to the session created by SAML SSO. Leave blank if there is no custom data to pass.

Onboard New Users

Don't create users during the SAML Single Sign On process.

Yellowfin can be configured to create new user accounts for any user who does not already exist in the system. This feature is called “onboarding”, and requires some additional configuration to provide Yellowfin with the information required to create new users from a SAML request. All of the following parameters must be set up and configured in the identity provider and Yellowfin to match the other attribute mapping parameters above.

Parameter	Description	Required?	Default
First Name Attribute	This parameter defines the name of the SAML attribute for fetching the first name for a new user.	Required	None
Last Name Attribute	This parameter defines the name of the SAML attribute for fetching the last name for a new user.	Required	None
Email Attribute	This parameter defines the name of the SAML attribute for fetching the email address for a new user.	Required	None
Language Code Attribute	The parameter defines the name of the SAML attribute for fetching the language code for a new user. The content of the SAML response should match an existing language code that has already been configured in the regional settings of the admin console. Language codes are the standard ISO format, with two characters for the language, and if required, an underscore and two more characters for the country (for example, nl for Dutch, or fr_ch for Swiss French).	Not required	System default
Password Attribute	The parameter defines the name of the SAML attribute for fetching the password for a new user. If left blank, a random password will be created for the user.	Not required	Random password (32 alphanumeric string)
Role Attribute	This parameter defines the name of the SAML attribute for fetching the role for a new user. If omitted, the default role will be given to the new user. The content of the SAML response should match an existing role code that has already been configured in the admin console.	Not required	Default role
Fallback Role	This dropdown list provides the means of selecting a fallback role if the role entered in the Role Attribute field is not available at the time of provisioning a new user. If omitted, the default role will be given to the new user.	Not required	Default role

To configure SAML onboarding, follow the steps below.

1. Ensure you're in the same configuration screen described in the preceding steps
2. Click on the **Onboard New Users** toggle to enable it

Onboard New Users

Create users with information from the SAML request if they don't already exist during the Single Sign On process.

First Name Attribute

Enter the SAML attribute that holds the value of the user's first name. This is used to provision a user when onboarding is enabled.

Last Name Attribute

Enter the SAML attribute that holds the value of the user's last name. This is used to provision a user when onboarding is enabled.

Email Attribute

Enter the SAML attribute that holds the value of the user's email address. This is used to provision a user when onboarding is enabled.

Language Code Attribute

Enter the SAML attribute that holds the value of the user's language code. This can be used to provision a user when onboarding is enabled. This can be left blank.

Password Attribute

Enter the SAML attribute that holds the value of the user's password. This can be used to provision a user when onboarding is enabled. If left blank, a random password will be assigned to the user upon creation.

Role Attribute

Enter the SAML attribute that holds the value of the user's role. This can be used to provision a user when onboarding is enabled. If the role defined here is not found, the Fallback Role field, below, will be used. If left blank, the default role will be given to the user.

Fallback Role

Enter the role that a user will receive if the Role Attribute field, defined above, is not present in a user's SAML attributes. If left blank, the default role will be given to the user.

-- Select --

Client Organizations

Password Settings

3. Refer to the preceding table to enter values for the required fields: **First Name Attribute**, **Last Name Attribute** and **Email Attribute**

4. Refer to the preceding table to enter any other values for the other, non-mandatory fields described (see the image below for an example)

Onboard New Users

Create users with information from the SAML request if they don't already exist during the Single Sign On process.

First Name Attribute

Enter the SAML attribute that holds the value of the user's first name. This is used to provision a user when onboarding is enabled.

first_name

Last Name Attribute

Enter the SAML attribute that holds the value of the user's last name. This is used to provision a user when onboarding is enabled.

last_name

Email Attribute

Enter the SAML attribute that holds the value of the user's email address. This is used to provision a user when onboarding is enabled.

email

Language Code Attribute

Enter the SAML attribute that holds the value of the user's language code. This can be used to provision a user when onboarding is enabled. This can be left blank.

en_au

Password Attribute

Enter the SAML attribute that holds the value of the user's password. This can be used to provision a user when onboarding is enabled. If left blank, a random password will be assigned to the user upon creation.

Role Attribute

Enter the SAML attribute that holds the value of the user's role. This can be used to provision a user when onboarding is enabled. If the role defined here is not found, the Fallback Role field, below, will be used. If left blank, the default role will be given to the user.

yf_role

Fallback Role

Enter the role that a user will receive if the Role Attribute field, defined above, is not present in a user's SAML attributes. If left blank, the default role will be given to the user.

Personal Content Writer & Collab... ▾

[top](#)

Customize data with CustomParameters and Parameters

If you already take advantage of the `CustomParameters` and `Parameters` options on an SSO web services call, these can also be added to SAML by using the fields `SSO Entry Options` and `SSO Custom Session Variable Attribute`.

SSO Entry Options

The `SSO Entry Options` Attribute field allows custom data per user that can be passed via the `CustomParameters` option on an SSO web service to be passed to a session created by the SAML SSO process. This is attribute based, so it can be applied to individual users.

The `SSO Entry Options` Attribute field allows custom session variables to be set on a per-session basis when using SAML Single Sign On. The attribute can contain webservice SSO Session Options that will be applied to the session created by the SAML SSO process.

For example, if you want a user to see their favourite reports, dashboards, stories and so on when they login, you could create a SAML attribute called `SsoOptions` with the `TIMELINE` and `DISABLEHEADER` parameters (or any others listed on the [Defining Login Session Options](#) wiki page). We'll use these for our example below.

1. In the **SAML Configuration** area of Yellowfin, locate the **SSO Entry Options Attribute** field
2. Type the name of your SAML attribute

SSO Entry Options Attribute

Enter the SAML attribute that holds the value of comma-separated webservice session parameters to pass to the session created by SAML SSO. Leave blank if there are no session parameters to pass.

SsoOptions

Custom Session Parameter Attribute

Enter the SAML attribute that holds the value of a custom variable to pass to the session created by SAML SSO. Leave blank if there is no custom data to pass.

3. Click the **Save** button to save your changes

You can test that your changes worked by logging in using your SAML token and checking that the login options you've specified are displayed.

Custom Session Parameter Attribute

The `Custom Session Parameter Attribute` field allows passing custom values to the resulting Yellowfin session when a user logs in via SAML. This is the same parameter that can be passed through via the 'Parameters' option on an SSO web service login. This is attribute based, so it can be applied to individual users.

To use this field, you will need to write your own Java plugin. Any number of variables can be passed to the Yellowfin session, so this can provide additional flexibility for custom requirements.

For example, if you wish to implement a custom header to replace the generic Yellowfin header, you could put a JSON array in this field that the header could extract information from to display at the top of the page. This could include user-specific details, such as their role, their photo or even links to the three most recent reports they've worked on.

In Yellowfin, the only requirement is to add those details to the Custom Session Parameter Attribute field.

[top](#)
