Single Sign On - SAML extension for LimeSurvey 6

version 1.7.0

Implemented by Sixto Martin Garcia
sixto.martin.garcia@gmail.com

Description **2**
How does it work? **4**
The usual use case, SP-initiated SSO flow 4
IdP-initiated SSO flow 5
IdP-initiated and SP-initiated SLO flow 5
Installation **6**
Dropping the Files 6
Settings **8**
Identity Provider section 9
Attribute Mapping section 11
Options section 12
Custom Messages section 14
Survey Protection SAML Settings 14
Global Permission section
In this section you determine what permission will be assigned to a new user created by the extension. 14
Advanced Settings section 15
Protect Survey Settings **19**
SP SAML Metadata **20**
FAQ **21**
Is there a demo or trial? 21
Is the extension compatible with IdP XXX? 21
When I try to SSO/JIT provision a user, I end in the Limesurvey page and not logged in? 21
The IdP returned that it has issues with the NameID Policy Format of the AuthNRequest? 22
I'm using ADFS, and when the Limesurvey SAML extension sends the AuthNRequest I experience an error on ADFS side 23
How can I know what user attributes are sent by the Identity Provider? 23
I'm blocked, I got an error in the SAML integration and don't know how to continue. 23
If I want to provide a cert/private key hosting it in the filesystem, where is the default path? 24
Can I place the SP cert/private key in another path? 24
Does the extension support Single Logout using HTTP-POST binding? 24
Is it secure to leave the strict parameter of the Advanced settings section disabled? 25
Is the extension secure? 25
Identity Providers supported **26**

Description

This is a Limesurvey extension that adds SAML Single Sign On support.

At the end of the SAML integration process we will be able to SSO and Just-in-time provisioning users in Limesurvey, verifying user credentials at the Identity Provider.

In a SAML integration, the Identity Provider and the Service provider exchange SAML Metadata (a XML file which contains its Entity ID (a name to identify the entity), SAML endpoints (where SAML Messages are generated or processed) and x509 certificates and private keys, to be able to sign/validate and encrypt/decrypt SAML Messages.

When an IdP and an SP exchange the metadata and register it, the circle of trust is done, and then the SP will trust the user info provided by the Identity Provider (after processing the SAML Message and validating it)

In the Identity Providers supported section of this document, you can find links to documentation that describes how to register a Service Provider at some of the supported Identity Providers

The SAML extension To be able to SSO only requires the Identity Provider to include in the SAMLResponse the email (or in case of using a custom attribute to identify users, that field).

To create user accounts, the extension requires the Identity Provider to provide user data, the minimum data required is limited by the LimeSurvey platform itself when registering a new user: username, email, fullname and group.

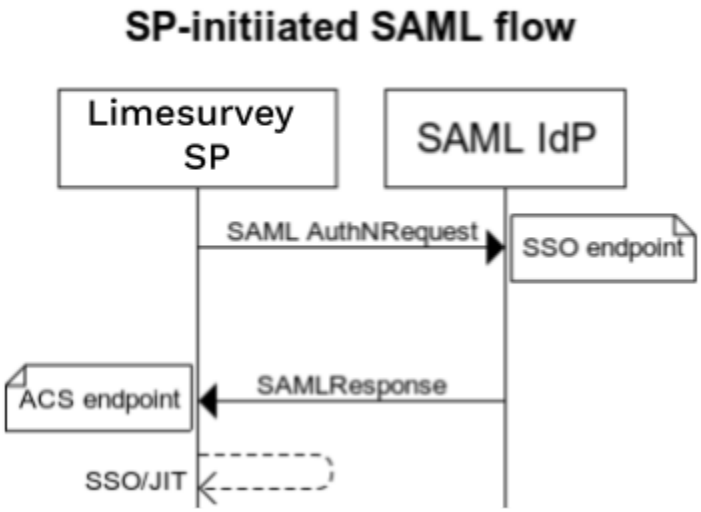
Each Identity provider names the user attributes differently so it is important to set a relation between the name of the user attributes provided by the IdP and the name of the fields at LimeSurvey. That relation is described in the “Attribute Mapping” section.

How does it work?

The usual use case, SP-initiated SSO flow

The extension adds a link "Login via Identity provider", which is customizable at the customer login form page.

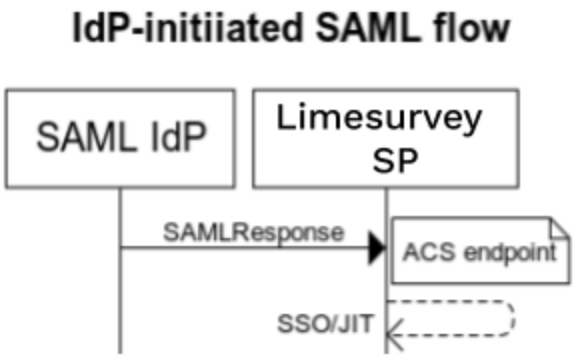
Following the link initiates a series of redirects that are described by the
SAML 2.0 standard.



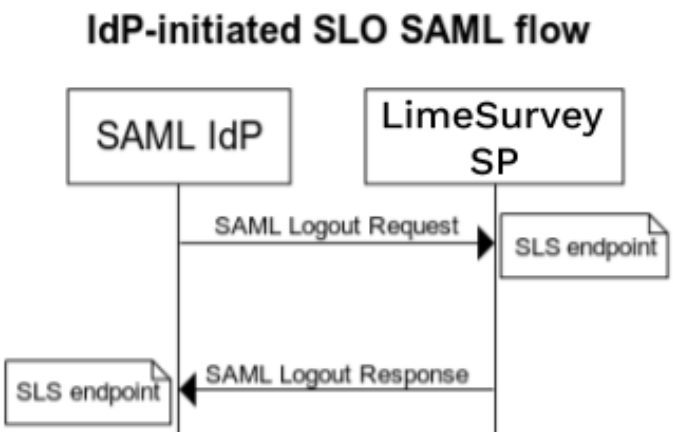
A SAMLRequest is sent to the Identity Provider, customer authenticates against the SAML Identity Provider and then information about user, is sent to LimeSurvey in a SAMLResponse, LimeSurvey SAML extension validates the SAMLResponse, authenticate customer (provisioning it if does not exists and that feature is enabled and let him in.

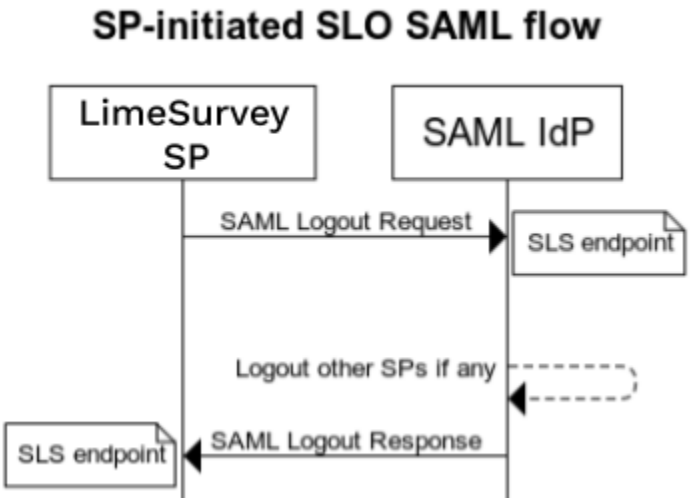
IdP-initiated SSO flow

The extension supports IdP-Initiated flow. A SAML Response can be directly sent by the Identity Provider and processed by the LimeSurvey SAML extension.



IdP-initiated and SP-initiated SLO flow





Installation

The SAML extension uses php-saml 4.X (PHP 7.4, PHP 8.X) so make sure to satisfy its dependencies, and some core extensions like php-xml, php-date, php-zlib. openssl. Install the OpenSSL library. It handles x509 certificates.

There are 2 ways to install the extension:

- Unzip and drop the files in the plugins folder
- Use the plugin Manager

Dropping the Files

Copy the **AuthSAML2** folder, which you will find after unzip the provided file, inside the **plugins** folder of LimeSurvey.

Now go to the Admin panel, **Settings > Plugin Manager** then click on **Scan files, AuthSaml2** should appear, click on its install icon.

Plugin Manager

In order to install the plugin go to the Admin panel. Then, access **Settings > Plugin Manager**, click on the **Upload & Install** button and select the provided zip file.

But previously, you needed to whitelist the “xsd” extension, editing the file application/config/config-defaults.php

And searching the var $config['allowedpluginuploads'], adding “xsd”.

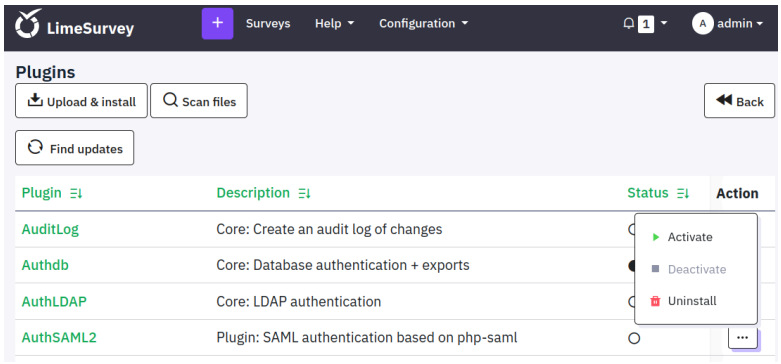
Example: $config['allowedpluginuploads'] = 'gif,ico,jpg,png,css,js,map,json,eot,otf,ttf,woff,txt,md,xml,woff2,twig,php,html,po,mo,xsd';

Otherwise, the Plugin Manager will not install the required xsd files, used to validate the SAML XMLs, and you will need to install them manually.

Settings

To configure the plugin go to the Admin panel. Then access to **Settings > Plugin Manager,** and you will see the **AuthSAML2** listed.

If it is not listed, click on **Scan Files** and a view will appear where you will be able to install the extension to be recognized.



If you see the extension on the list, click on its name to access its setting configuration panel. After this process, we can go back to this list and click on the dots and select “Activate” to enable the extension.

In the Settings panel, there are several sections:

- **Service Provider Metadata**. Contains a link to the SP metadata
- **Identity Provider settings**. Set parameters related to the IdP/IdPs that will be connected with our LimeSurvey.
- **Mappings**. Set the mapping between IdP fields and LimeSurvey user fields.
- **Options**. Configure the behaviour of the extension.
- **Survey Protection SAML Settings.** Contains the flag **Surveys protected by login and others,** which allows the survey administrators

to force all survey participants to be authenticated, and other requirements

- **Global Permissions**. To handle the permissions that will be assigned to the new user.
- **Advanced SAML Settings**. To configure SAML security settings

Service Provider Metadata

The **Metadata Link** is very important for the SAML integration, if you click on it you will be redirected to the SP Metadata endpoint, a view that provides the XML file that defines the Service Provider (extension needs to be enabled).

You will need to provide the URL or the content of that XML to the Identity Provider administrator to register it at the Identity Provider.

If you are using multiple IdPs, take in mind that each IdP registered will be related to its own SP so add to the SP Metadata URL at the end the /idp/{idp_index}

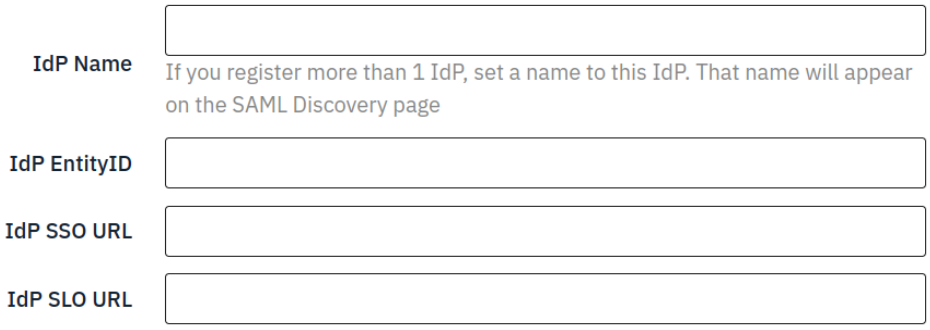
```
index.php/plugins/direct/plugin/AuthSAML2/function/samlmetadata/idp/1
```

Identity Provider section

Here you set some info related to the IdP that will be connected with our LimeSurvey. Contact the administrator of the IdP and ask him for the IdP metadata XML, which will contain the data to include in this section.

There are fields in the case that you will use 1 unique IdP and another Json field where you can set multiple IdPs (**Multiple IdP support** field).

Find a link to the **Importer IdP view** to directly paste the XML and process it to be included as the default IdP, or the extra multi-mode IdP.

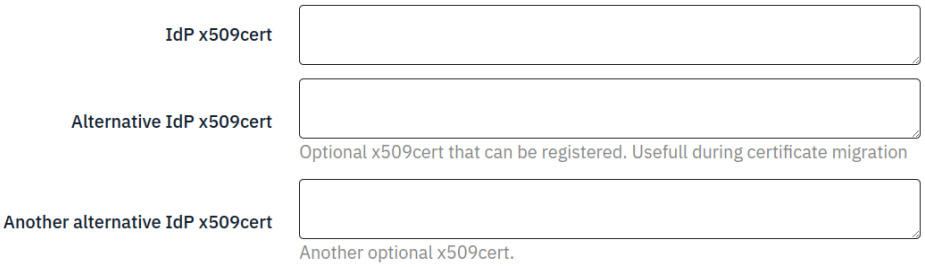


The **IdP Entity Id** is the identifier of the IdP, the EntityID value in the XML of the IdP metadata.

The **Single Sign On Service Url** and the **Single Log Out Service Url** are the IdP endpoints that will process the SAML Messages generated by the LimeSurvey SAML extension.
The first one is used on the SSO flow to process AuthNRequests, the second one processes LogoutRequest or LogoutResponses generated by the LimeSurvey SAML extension.

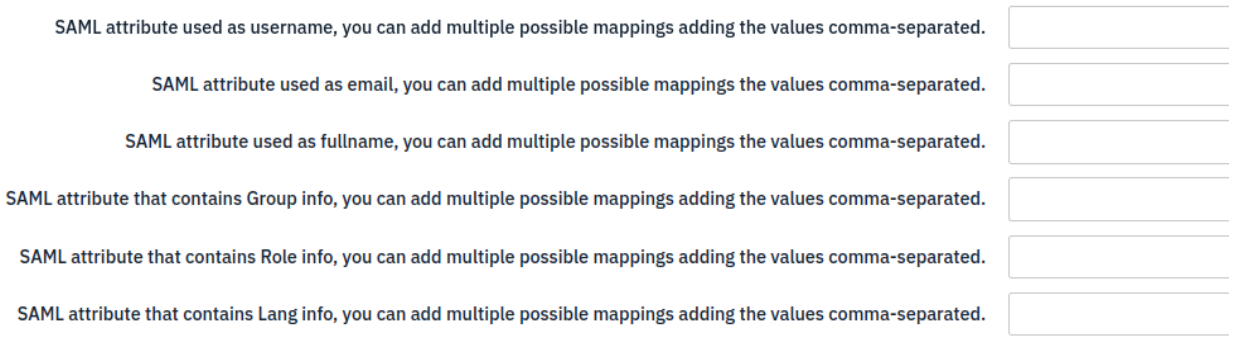
The **X.509 Certificate** and the rest of certs fields store x509 certs used by the Identity Provider and the LimeSurvey SAML Extension uses it to validate the Signature of the SAML Messages received. Only the first

cert is used by the LimeSurvey SAML extension to encrypt any element.



Attribute Mapping section

Sometimes, the names of the attributes sent by the IdP do not match those used by LimeSurvey for the customer accounts. In this section, we must set the mapping between IdP fields and LimeSurvey fields. You can set different possible mappings for each attribute that gonna be mapped, comma-separating them. Order matters: if there is a saml attribute that matches, it is retrieved, no other mappings are considered for that attribute. If multiple IdPs are registered, add all the possible mappings for each attribute. Is support comma-separated values.



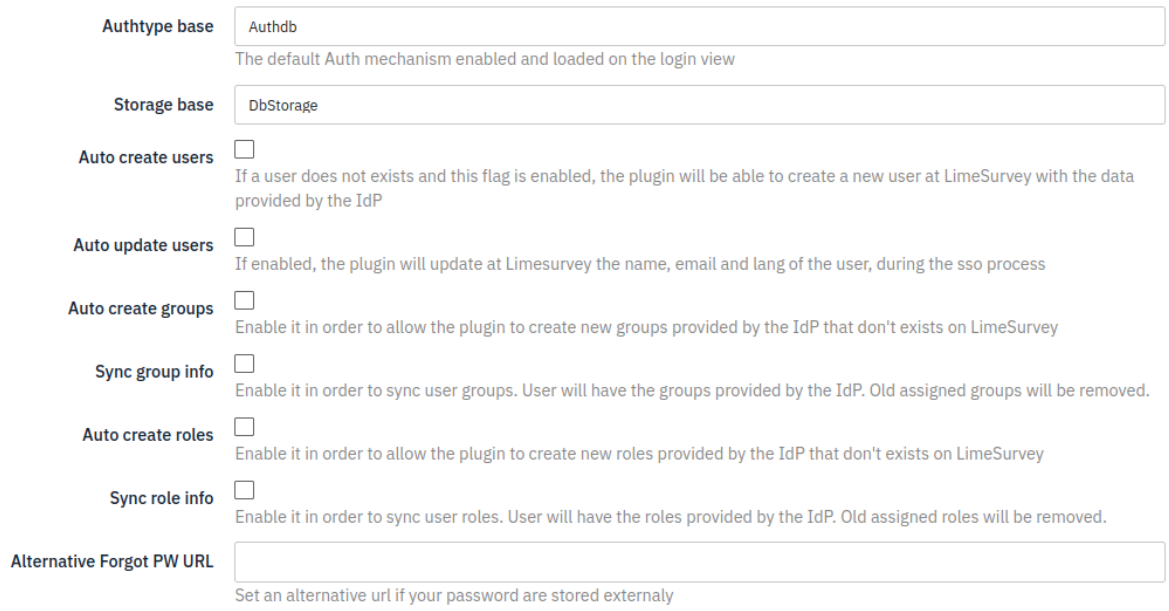
Options section

In this section we determine some behaviours of the extension.

Leave **AuthType base** and **Storage base** as the default value if you are using the default installation and set any other value if you are using another AuthType to identify users or a different way to store data.

We enable/disable JIT provisioning (auto-create user accounts) by the **Auto create users** field.

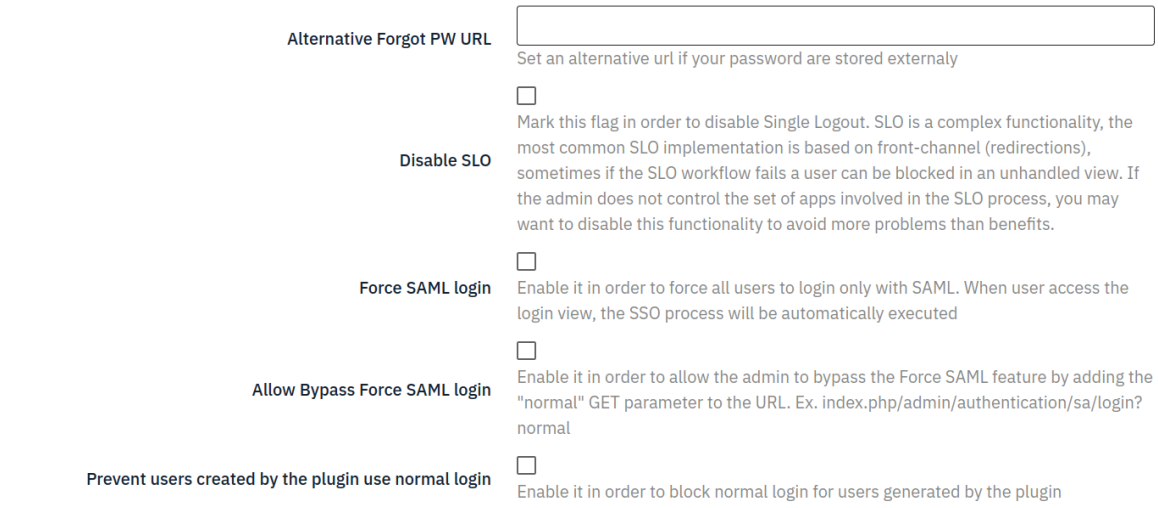
If you want to sync the user data hosted on the IdP in the LimeSurvey user account, then enable the **Auto update users** field setting.



The extension supports Groups. If the IdP provides a group name that not exists yet, you can enable **Sync group info** field to generate it automatically. It also supports Roles, which can also be autocreated and synchronized.

And to set an **Alternative Forgot PW URL** to be able to redirect the

users to the IdP forgot password url and stop using the limesurvey forgot password feature.



Single Log Out (SLO) is a complex functionality, the most common SLO implementation is based on front-channel (redirections), sometimes if the SLO workflow fails, a user can be blocked in an unhandled view. If the admin does not control the set of apps involved in the SLO process, maybe it is better to disable this functionality as it could carry more problems than benefits. **Disable SLO** enable/disable it.

You can force users when accessing the login view to be automatically redirected to initiate the SAML SSO flow, by enabling the **Force SAML login** setting.

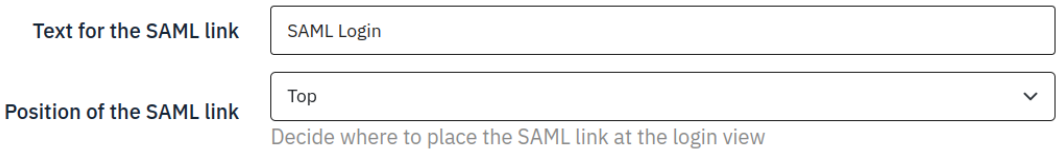
Sometimes when **Force SAML login** is enabled, it makes sense to have a way to bypass it when the SAML integration is not working to recover the system. You can with the field **Allow Bypass Force SAML login** enable the option to append to the login view the '?normal' parameter to be able login with the standard Auth method.

There Is also a setting to force all users created by the extension to authenticate using SAML and forbids its use of the standard login.

The **IdP Discover method** allows you to decide, in case that more than 1 IdP is registered in the LimeSurvey instance, how to do the IdP discovery. You can present a list with the IdP names, IdP Entity Ids or implement your way of selecting the IdP using the custom option.

Custom Messages section

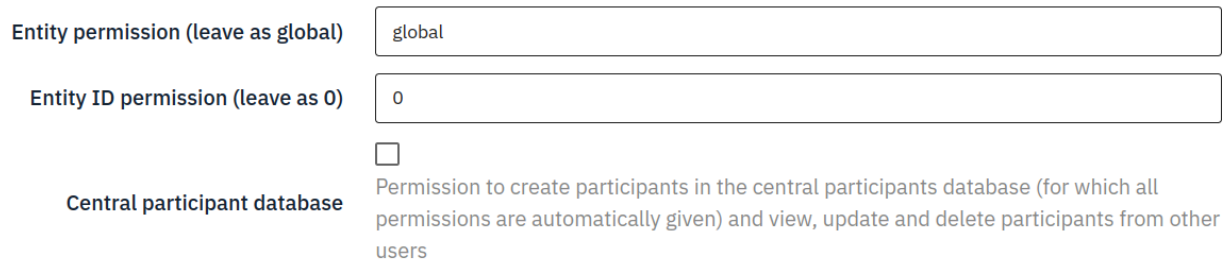
Handle what text is shown in the login form and where to position it.

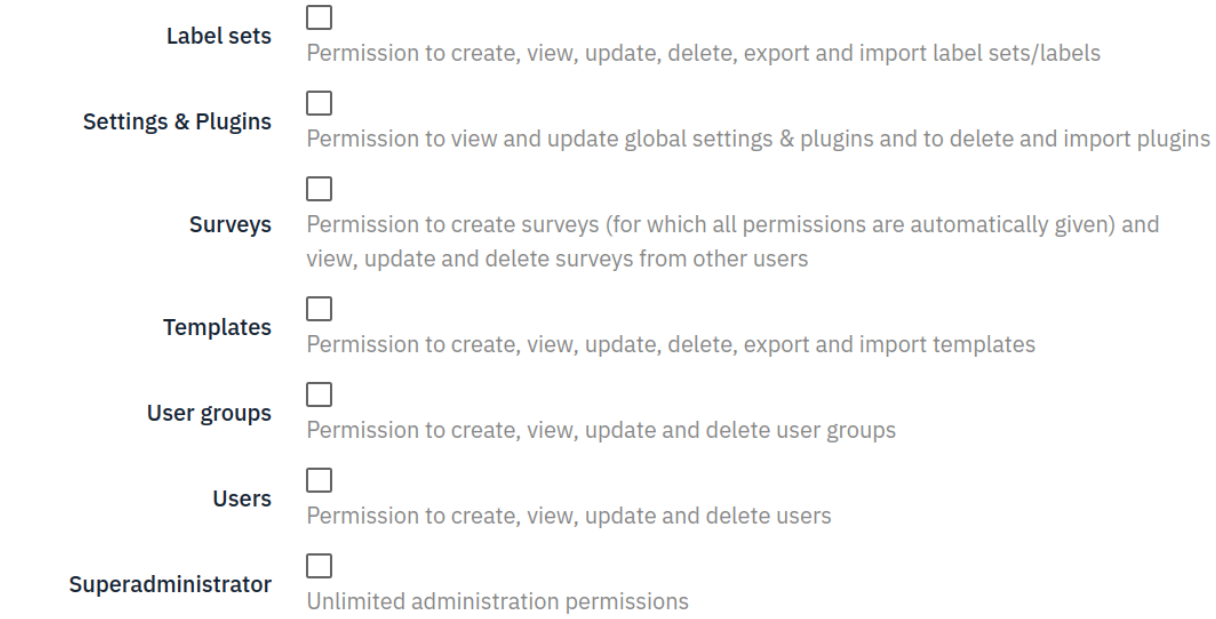


Survey Protection SAML Settings

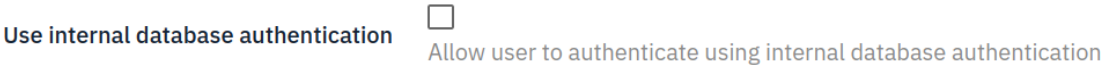
Global Permission section

In this section you determine what permission will be assigned to a new user created by the extension.





And there is also a field to allow users to keep using the internal database, which should be enabled if Force SAML is disabled.



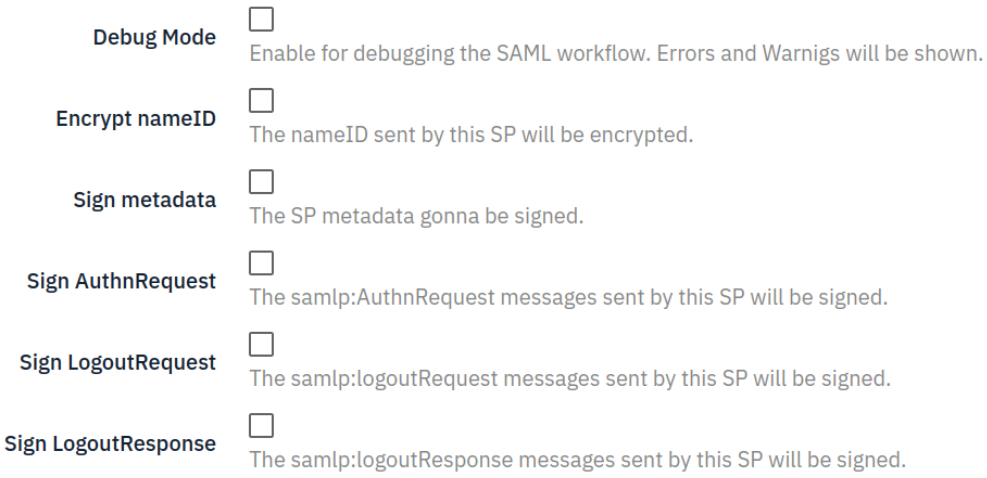
Advanced Settings section

Handle some other parameters related to customizations and security issues. Most of the settings belong to the advanced settings of the php-saml toolkit

If sign/encryption is enabled, then x509 cert and private key for the SP must be provided. There are 2 ways:

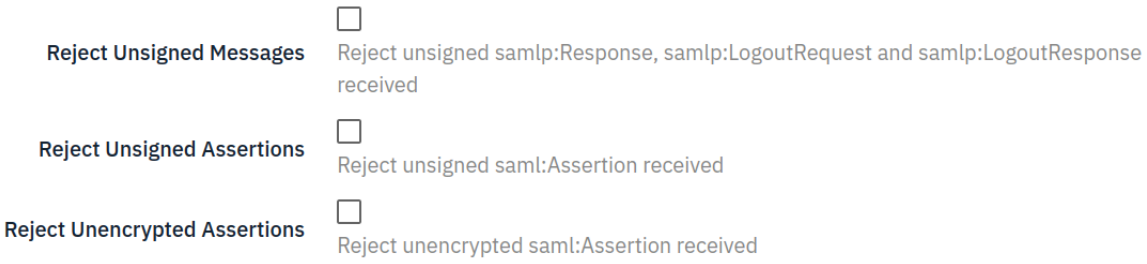
1. Store them as files named sp.key and sp.crt on the 'certs' folder of the extension. (Be sure that the folder is protected and not exposed to the internet)

2. Store them in the database, filling the corresponding textareas. (Take care of security issues)

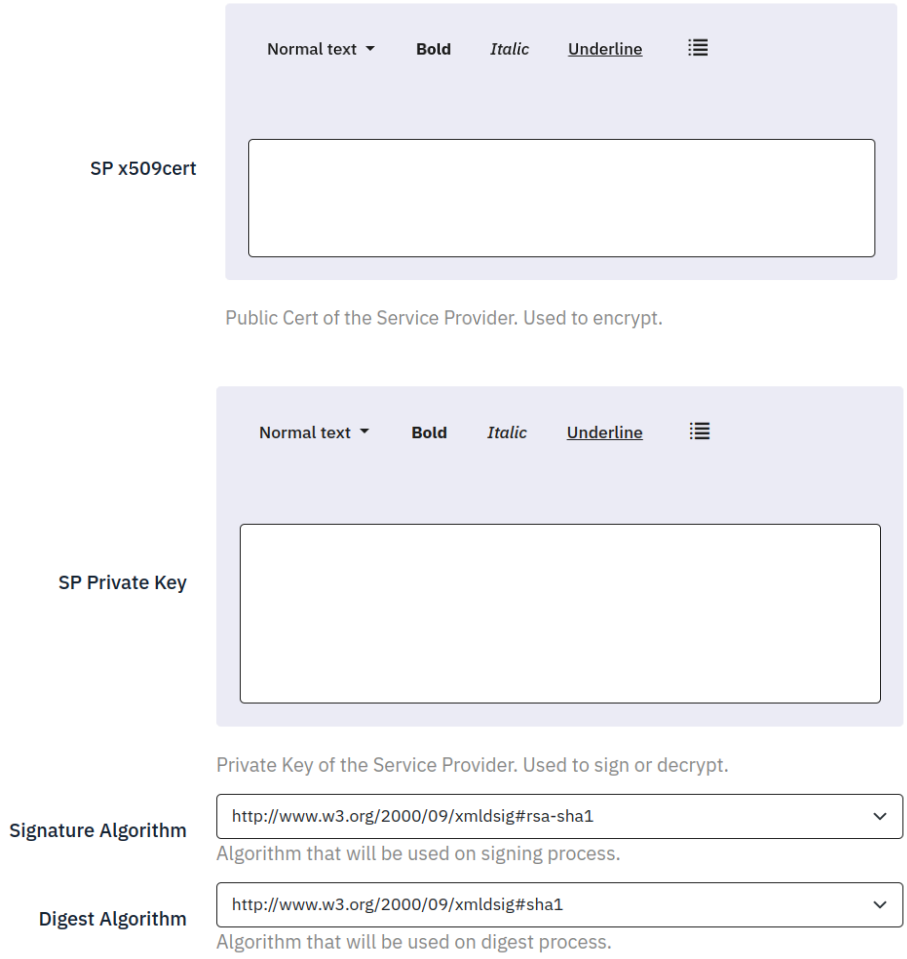


While configuring the SAML integration, you should enable the **Debug Mode** so the extension in case of rejecting the SAMLResponse will provide its cause.

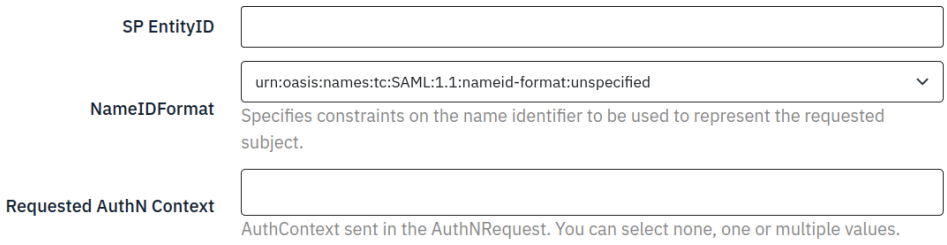
If the Identity Provider requires it, you can enable Signatures on AuthNRequest, LogoutRequest and LogoutResponses, as well as require signatures on SAML messages or encrypted SAMLResponses. There are flags that control this.



If you enable signatures on the SP, you will need to provide **SP Private Key** and SP **Public certificate**, and you can decide the Sign and Digest Algorithm

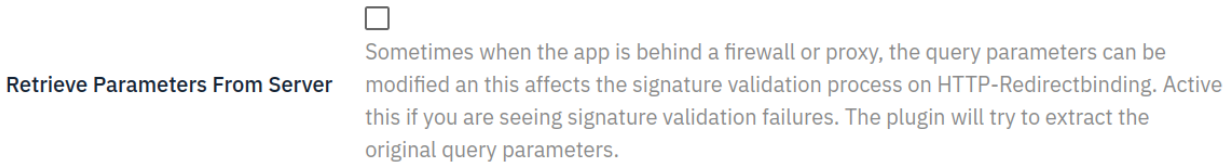


You can set a specific Entity ID for the SP, if you don't provide it, the URL where the SP Metadata is published is used as Entity ID.



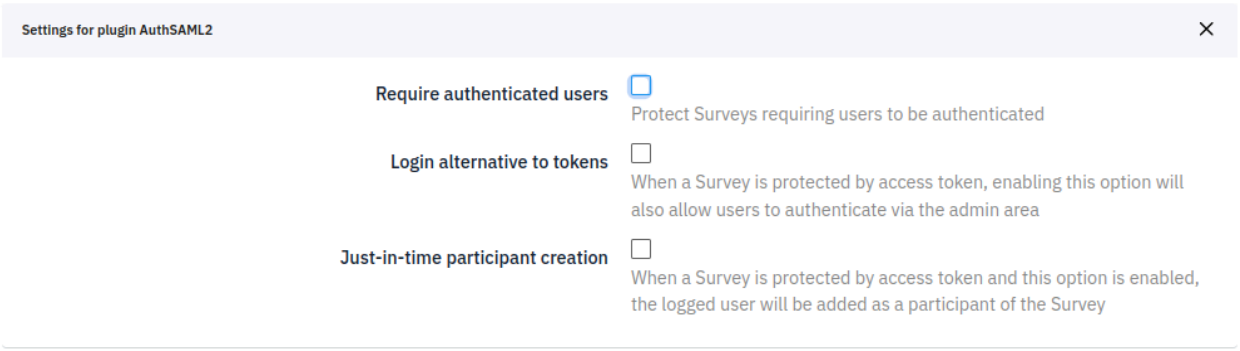
You may review what NameID Format and what AuthNContext are supported by the Identity Provider and set it correctly on the settings.

When the SP is behind a firewall or load balancer and the URL retrieved by the toolkit is wrong, you can enable the Retrieve Parameters From Server flag to make the toolkit aware of that fact and allow it.



Protect Survey Settings

When the **Surveys protected by login and others** flag of the **Survey Protection SAML Settings** is enabled, at the Survey Admin view, you will be able to find at the “Simple plugins” section the following Setting panel:



This allows the admin to decide whether to enable or not additional ways to protect/authenticate participants.

If the admin wants to force users to be logged in to participate in a survey, enable **Require authenticated users**

On surveys protected by tokens, you can enable **Login alternative to tokens** to offer a login link in the token view, as an alternative to providing a token. When this option is enabled and a user is logged in, the SAML extension will automatically fetch the token if the user's email is registered already as a participant. If it is not yet a participant, the flag **Just-in-time participant creation** needs to be enabled to automatically register the user as a participant.

SP SAML Metadata

The metadata of the LimeSurvey Service Provider will be available at:

<limesurvey_base_url>/index.php/plugins/direct/plugin/AuthSAML2/function/samlmetadata + [idp/ {idp_index }]

FAQ

Is there a demo or trial?

There is no demo side or trial code.

Is the extension compatible with IdP XXX?

The extension is compatible with any Identity Provider that supports SAML 2.0, see list of the Identity Providers that already were used with the extension.

Can I have commercial support?

Yes I offer commercial support as well that you can pay via Paypal.
Rate 50€/h. You can use this to solve doubts, get help with the installation or configuration ,as well as implement customizations.

When using the SAML extension, I got a 500 error/white page

You may review the Server/PHP logs to check what's going on.

When I try to SSO/JIT provision a user, I end in the Limesurvey page and not logged in?

There are some possible reasons for not being logged in:

- The IdP returned a SAMLResponse with status different than Success, which indicates that the AuthNRequest was rejected.
- The SAMLResponse was invalidated
- The extension was not able to SSO/JiT the user due a lack of user data or due invalid values.

In the Advanced settings section, you can find a **debug** boolean field that you can enable in order to record the reason of the error on the error trace. Be sure to enable it, reply to the SSO process and check the errors registered on the PHP logs.

If the SAMLResponse contains a SAMLResponse with a bad status, ask the Identity Provider administrator why the AuthNRequest was rejected.

If the SAMLResponse was rejected, you will see that message as well as the reason for the rejection. You will need to review the settings on the IdP and SP sides to validate.

If the cause mentions something related to Signature invalidation, review the x509cert of the IdP registered, verify that the value matches the ds:X509Certificate included in the SAMLResponse.

If the error is related to user login or user account creation, review that the required account is provided by the IdP, review that the mappings are correct and also that the data is valid.

The IdP returned that it has issues with the NameID Policy Format of the AuthNRequest?

In the Advanced settings section, you have a **Name ID Format** select field with several alternatives. The one selected needs to be aligned

with the NameID Formats supported by the IdP (which is sometimes exposed in the IdP SAML metadata). If you are unsure what to set, configure it as unspecified, otherwise, emailAddress used to be the most common value.

I'm using ADFS, and when the Limesurvey SAML extension sends the AuthNRequest I experience an error on ADFS side

Many possible issues could happen, the first approach is to review error logs of ADFS to try identify the cause of the error. You can Google the ID or the message of the error that appears on the error log to try to find a solution.

How can I know what user attributes are sent by the Identity Provider?

There Is a Firefox extension named SAMLTracer that you can use in order to record the SAML flow between the IdP and the SP in order to record the SAMLResponse and analyze it to see the AttributeStatement. Check SAMLTracer how-to.
Chrome users can use Chrome SAML Panel.

I'm blocked, I got an error in the SAML integration and don't know how to continue.

Contact me by mail and provide:
- A description of what you get and what was expected.

- A SAMLTrace log (the tool allows you to export the trace).
- A screenshot of the involved SAML settings (IdP and SP side).

I will try to determine the cause and provide you with a solution.

If required, we can schedule a video meeting if the resolution seems complex.

If I want to provide a cert/private key hosting it in the filesystem, where is the default path?

It depends on how you have installed the php-saml library, the default path is in the **certs** folder that you should find in the root of the php-saml folder. If you used composer, it should be at <limesurvey_root_folder>/plugins/AuthSAML2/certs

Can I place the SP cert/private key in another path?

Yes, you can define in the PHP code a ONELOGIN_CUSTOMPATH filesystem path, and the php-saml library will expect the **certs** folder on that path.

Does the extension support Single Logout using HTTP-POST binding?

No, only HTTP-Redirect binding is supported for SLO.

Is it secure to leave the strict parameter of the Advanced settings section disabled?

No, you MUST enable it always in production environments.

Is the extension secure?

The extension is based on the php-saml library which was audited and certificated by third party security companies. In addition, the code is open source so anyone can access the code and verify it.

If a critical security fix is needed, it will be provided asap by an official release on the marketplace and the customers will be notified by the email used to purchase the extension, and code could be provided by mail if required.

Bug-fixes, non-critical fixes, and new features will be provided in new releases available on the marketplace.

Identity Providers supported

- OneLogin
- Okta
- Auth0, Auth0 Enterprise
- ADFS
- Azure AD and Azure AD B2C
- Keycloak
- Salesforce
- Shibboleth
- simpleSAMLphp
- Google
- AWS SSO
- Centrify
- Forgerock (OpenAM)
- Ping Identity
- RSA
- IBM
- Oracle
- WSO2
- NetIQ
- SecureAuth
- Citrix Netscaler
- F5 BIG-IP

Links of the IdP listed carry you to its official documentation.