Single Sign On - SAML extension Matomo

LoginSaml 5.x

Description

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

At the end of the SAML integration process we will be able to SSO and Just-in-time provisioning users into Matomo, 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, in order 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 can be found links to documentation that describes how to register a Service Provider at some of the supported Identity Providers
The SAML extension In order to be able to SSO only requires the Identity Provider to include in the SAMLResponse the *email* or the *username*, depending on what value was set as *field to identify the user*.

In order to create user accounts, the extension requires the Identity Provider to provide the following user data: username, email and alias.

Each Identity provider names the user attributes in a different way 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 Matomo. That relation is described in the “Attribute Mapping” section.

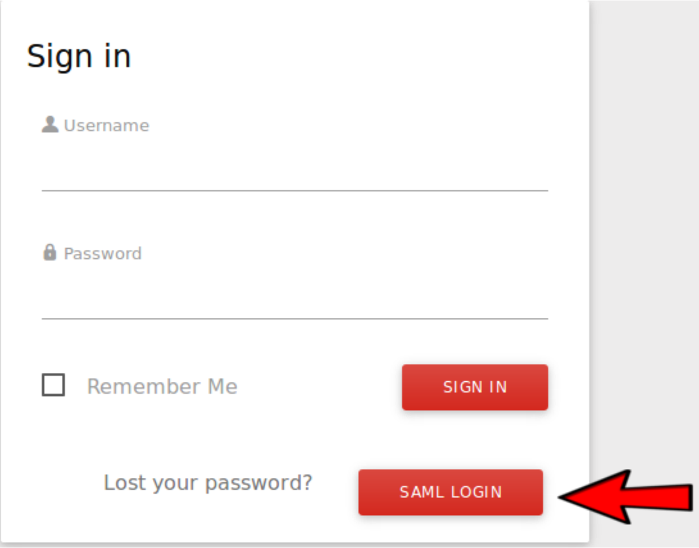
The extension also supports managing the level of access assigned to the user, configurable at the *Access Synchronization settings* section.

How does it work?

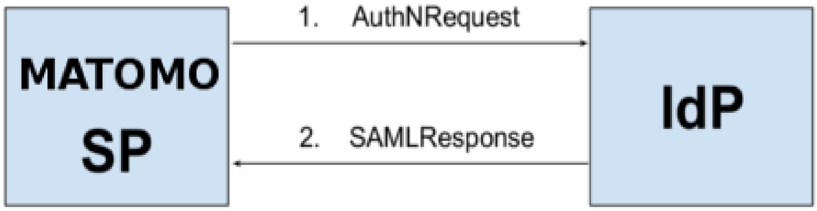
The normal use case, SP-initiated SSO flow

The extension adds a “SAML Login” link to the login form page.

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



If “Force SAML Login” is enabled, the login form will not be shown and the SP-initiated flow will start automatically.



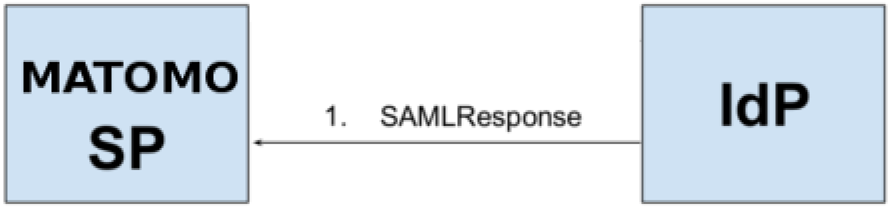
1. Redirect to Identity Provider (when “SAML Login” button on login screen is clicked):
    - Log message: Initiated the Single Sign On, Redirecting to the IdP (Log level: info)
2. When response from Identity Provider has come to Assertion Consumer Service endpoint:
    - Log message: Initiated the Assertion Consumer Service (Log level: info)
3. SAML validation successful:
    - Log message: SAMLResponse validated (Log level: info)
    - Log message: Attributes + NameId + NameIDFormat + SessionIndex (Log level: debug)
4. Or SAML validation returned some errors in response from Identity Provider:
    - Log message: SAMLResponse rejected. + Cause (Log level: error)
    - Log message: SAML Response XML (Log level: debug)
5. User creation (Optional step, if account was not found):
    - If user does not exist but Just-In-Time provisioning is enabled and required attributes are provided: Log message: Added user (Log level: info)

- If user has no default sites access: Log message: SAML settings does not define default sites to provide access to new users in ‘Options’ section (Log level: warning)
- If user has default sites access: Log message: Adding to user USER access to sites: SITES (Log level: info)
- If user does not exists and Just-In-Time provisioning is enabled but process has failed: Log message: Just-in-time provisioning error // X mapping is required // X was not provided (Log level: error)
- If user does not exists and Just-In-Time provisioning disabled: Log message: User does not exists and just-in-time provisioning is disabled (Log level: error)

6. Sync access (Optional step, if sync access enabled):
    - If the user has no data access: Log message: User has no access in SAML, but access synchronization is enabled. (Log level: warning)
    - If access data defines that user should be assigned as superuser: Log message: MatomoAccess synchronized. User is now superuser (Log level: info)
    - If access data defines user access on sites: *Log message**: MatomoAccess synched. Access of user updated (Log level: info)
7. Successful login:

- Log message: User with login authenticated in Matomo (Log level: info)

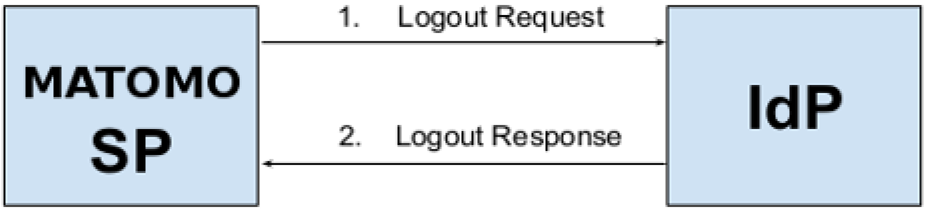
IdP-initiated SSO flow



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

Flow is similar to SP-initiated SSO but without step 1.

SP-initiated Single Logout authentication process (SLO enabled)

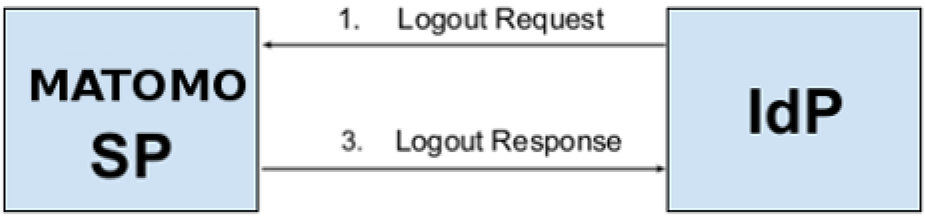


1. Redirect to Identity Provider. (Logout Request sent). When “logout” link clicked and user session initiated with SAML flow:
    - Log message: Initiated the Single Log Out for user with login USER (Log level: info)

2. When Logout Response from Identity Provider has come to Single Logout Service endpoint:
    - Log message: Initiated the Single Logout Service for user with login USER (Log level: info)
3. SAML validation:
    - If SAML Logout Response is valid: Log message: Single Logout Service executed. User with login USER logged out (Log level: info)
    - If there are some errors in Logout Response from Identity Provider: Log message: Error at Single Logout Service

endpoint. User with login USER. + Error reason (Log level: error)

IdP-initiated Single Logout authentication process (SLO enabled)



1. When Logout Request from Identity Provider has come to Single Logout Service endpoint:
    - Log message: Initiated the Single Logout Service for user with login USER (Log level: info)
2. SAML validation:
    - If there are some errors in Logout Request from Identity Provider: Log message: Error at Single Logout Service endpoint. User with login USER. + Error reason (Log level: error)
3. Redirect to Identity Provider (Logout Response sent)
4. When Logout Response from Identity Provider has come to Single Logout Service endpoint:

    - Log message: Initiated the Single Logout Service for user with login USER (Log level: info)
5. SAML validation is successful:
    - Log message: Single Logout Service executed. User with login USER logged out (Log level: info)
6. Or SAML validated failed: errors returned in Logout Response from Identity Provider:
    - Log message: Error at Single Logout Service endpoint. User with login USER. + Error reason (Log level: error)

Installation

The SAML extension uses php-saml 4.X so make sure to satisfy its dependencies. php >= 7.3 and some core extensions like php-xml, php-date, php-zlib. openssl. Install the openssl library. It handles x509 certificates.

Install the plugin according to Matomo's plugin installation guide.

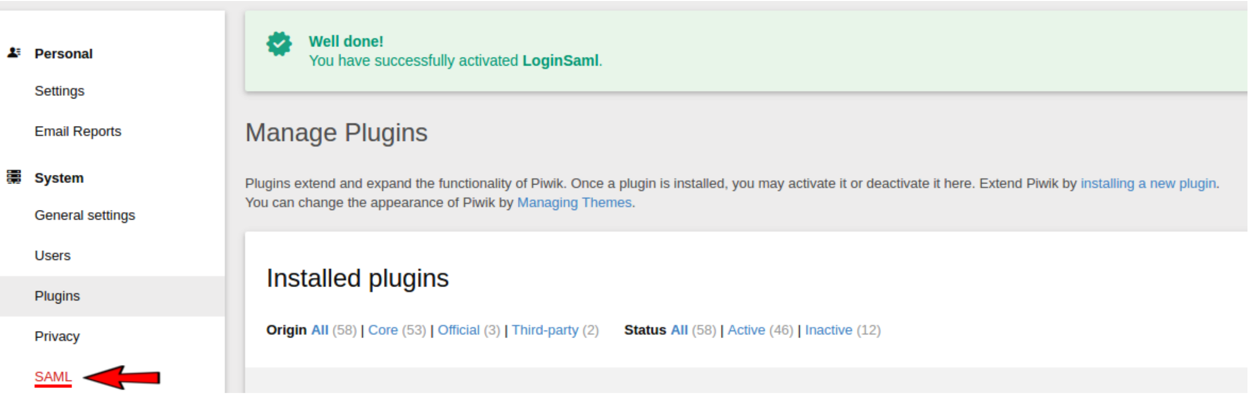
Configuration

To configure SAML authentication follow these steps:

1. Login as a Super User

2. On the Administration > Plugins page, activate the LoginSaml plugin.

3. Navigate to Settings > SAML page



Personal
Settings
Email Reports
System
General settings
Users
Plugins
Privacy
SAML

Well done!
You have successfully activated **LoginSaml**.

Manage Plugins

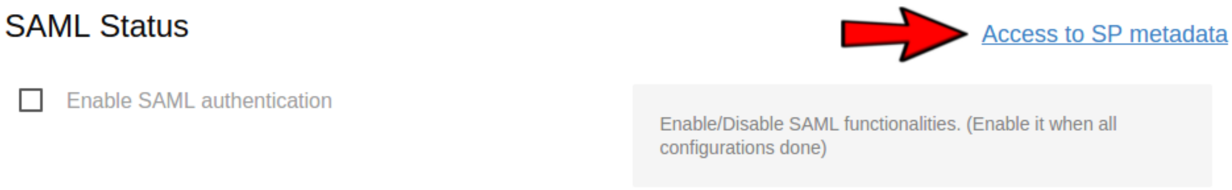
Plugins extend and expand the functionality of Piwik. Once a plugin is installed, you may activate it or deactivate it here. Extend Piwik by installing a new plugin.
You can change the appearance of Piwik by Managing Themes.

Installed plugins

Origin All (58) | Core (53) | Official (3) | Third-party (2) **Status** All (58) | Active (46) | Inactive (12)

4. Enter and save settings for SAML: add the Identity Provider info, set the attribute mappings and configure the other options as applicable.

5. Share Service Provider metadata with the IdP administrator



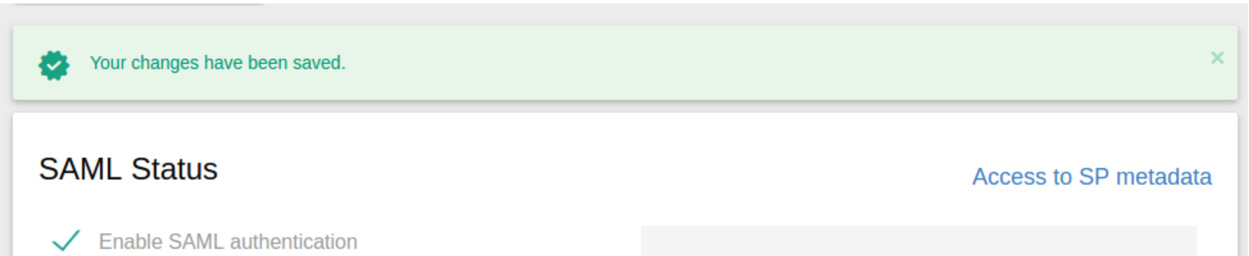
SAML Status

Access to SP metadata

□ Enable SAML authentication

Enable/Disable SAML functionalities. (Enable it when all configurations done)

6. Enable the SAML authentication



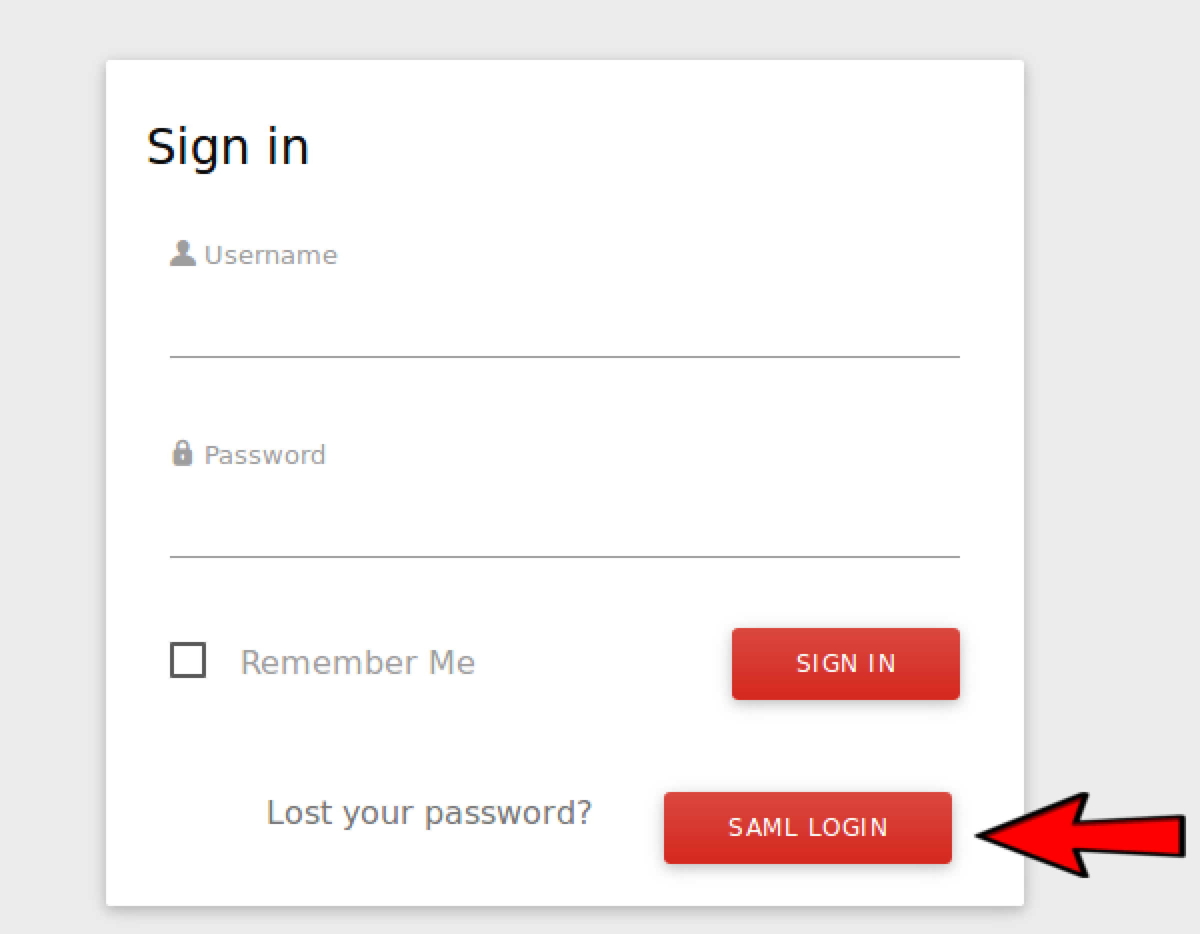
Your changes have been saved.

SAML Status

Access to SP metadata

✓ Enable SAML authentication

7. You can now open a new browser session and try to login with the SAML Identity Provider.

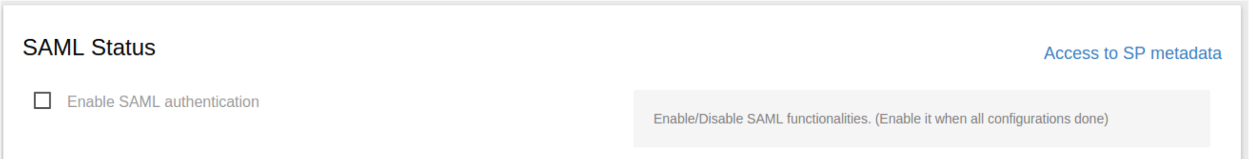


SAML Configuration support

Configuring SAML Authentication properly can be difficult so we offer our services to help you get Matomo Analytics (formerly Piwik Analytics) successfully working with SAML and enjoy the great benefits of SSO. Learn more and contact us in the SAML Support page.

Status section

Once you activate the SAML plugin, you are able to access its settings panel.



SAML Status

Access to SP metadata

□ Enable SAML authentication

Enable/Disable SAML functionalities. (Enable it when all configurations done)

In the Status Settings section you see Enable SAML authentication is disabled. When disabled, all SAML actions are disabled and if a user tries to execute them, she will receive an error notifying that the SAML functionality is disabled.

You may only enable it when the rest of the SAML settings are properly configured.

In SAML, there are 2 different kind of entities:

1. the Identity Providers IdP (the 3rd party entity where the user is authenticated), and

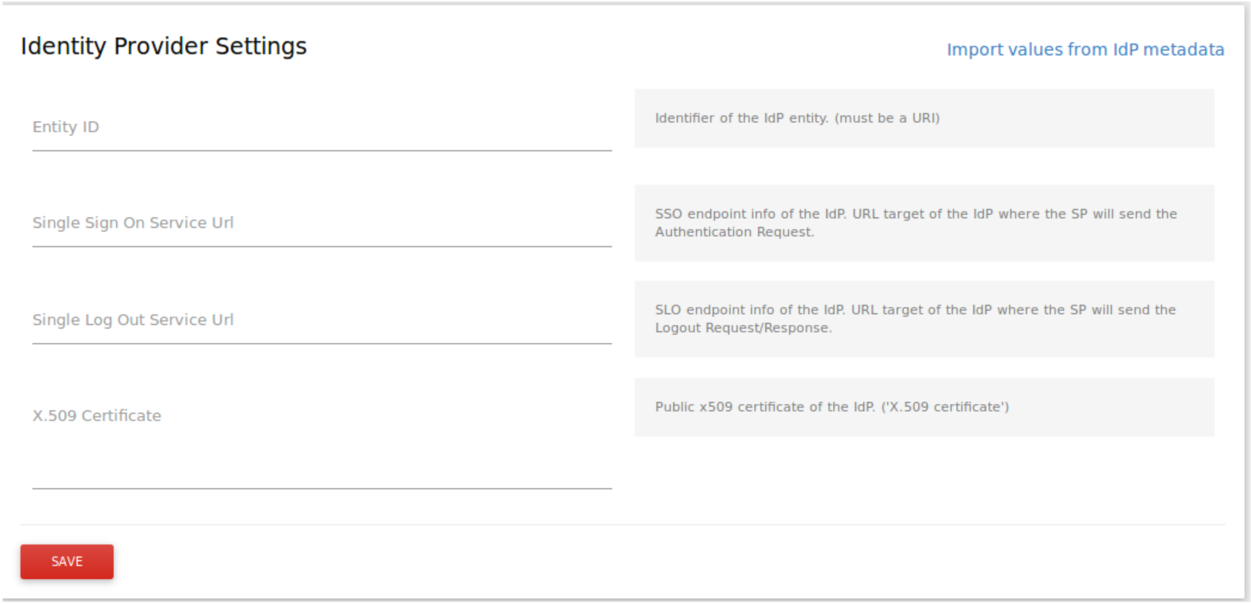
2. the Service Provider SP (the service that protects the app, in this case Matomo).

A circle of trust is defined between IdP and the SP, allowing all IdP users to access the SP under some conditions. That circle of trust is based on the exchange of an XML, named metadata, that describes the Entity ID, the entity endpoints and the public certificates (that will allow validation of signed/encrypted SAML messages).

Identity Provider Settings

In the Identity Provider Settings section, you may register the Identity Provider metadata.

You can directly fill the form:

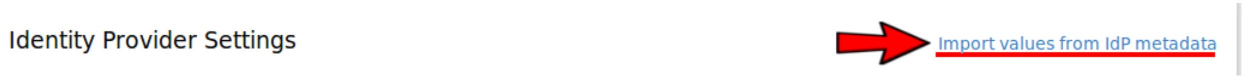


Identity Provider Settings

Import values from IdP metadata

Entity ID	Identifier of the IdP entity. (must be a URI)
Single Sign On Service Url	SSO endpoint info of the IdP. URL target of the IdP where the SP will send the Authentication Request.
Single Log Out Service Url	SLO endpoint info of the IdP. URL target of the IdP where the SP will send the Logout Request/Response.
X.509 Certificate	Public x509 certificate of the IdP. ('X.509 certificate')

or click on the Import values from IdP metadata link:



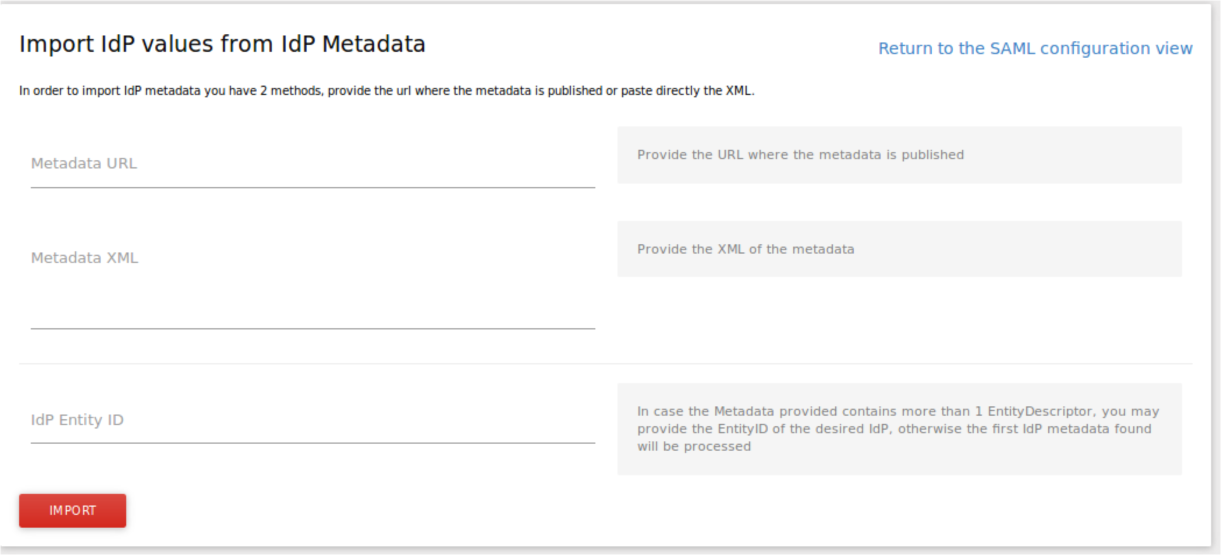
Identity Provider Settings

Import values from IdP metadata

This link will redirect to a form where two different methods are offered to let you import the Identity Provider metadata:

1. By metadata URL
2. By string XML

In case the imported metadata contains more than 1 Identity Provider entity description, you can use the IdP entity ID to identity the desired entity:



Import IdP values from IdP Metadata

Return to the SAML configuration view

In order to import IdP metadata you have 2 methods, provide the url where the metadata is published or paste directly the XML.

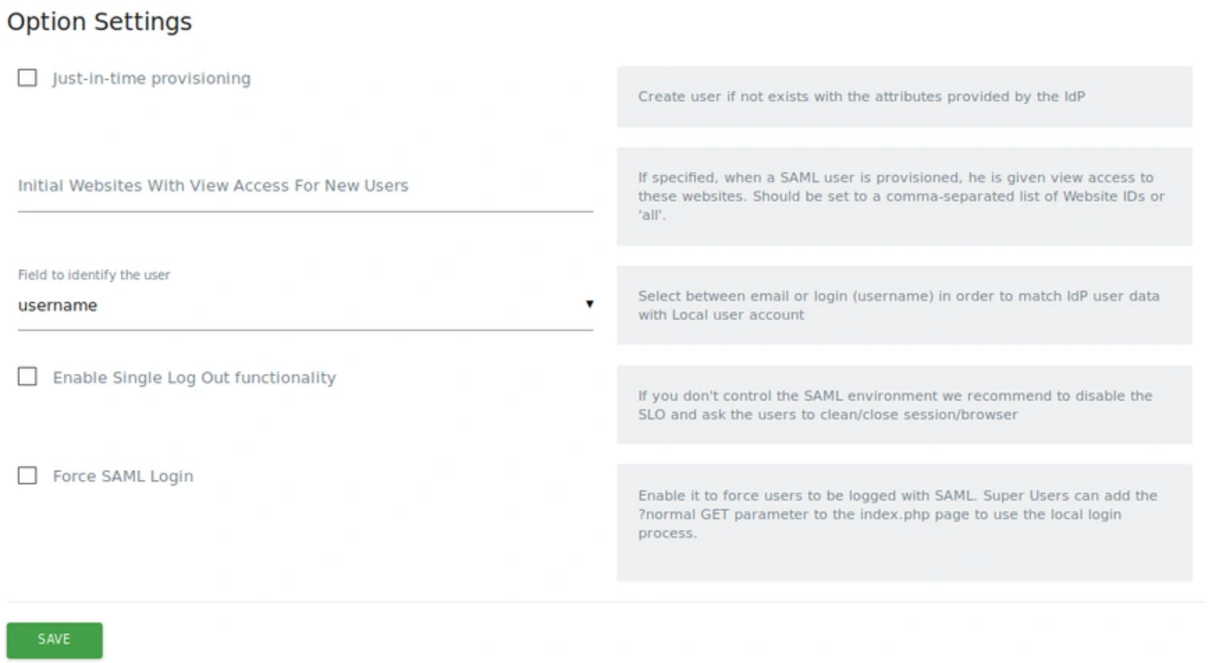
Metadata URL — Provide the URL where the metadata is published

Metadata XML — Provide the XML of the metadata

IdP Entity ID — In case the Metadata provided contains more than 1 EntityDescriptor, you may provide the EntityID of the desired IdP, otherwise the first IdP metadata found will be processed

Options settings

In the Option settings section you can define how Matomo SAML integration will act.



Option Settings

☐ Just-in-time provisioning

Create user if not exists with the attributes provided by the IdP

Initial Websites With View Access For New Users

If specified, when a SAML user is provisioned, he is given view access to these websites. Should be set to a comma-separated list of Website IDs or 'all'.

Field to identify the user

username ▾

Select between email or login (username) in order to match IdP user data with Local user account

☐ Enable Single Log Out functionality

If you don't control the SAML environment we recommend to disable the SLO and ask the users to clean/close session/browser

☐ Force SAML Login

Enable it to force users to be logged with SAML. Super Users can add the ?normal GET parameter to the index.php page to use the local login process.

In some scenarios it makes sense to enable the Just-in-time provisioning when you want to automatically create user accounts based on the data provided by the Identity Provider on the SAMLResponse.

If just-in-time provisioning is disabled or the required user data is not provided, an error will happen during the SSO process since we will not be able to initiate any Matomo account.

If just-in-time provisioning is enabled, by default any new users (created with just-in-time provisioning) will have no access to Matomo. You may set a default view permission (What is the 'view' permission in Matomo?) to some Matomo websites. Use the Initial sites with view access for new users to set a list of the Matomo Website IDs that the users will be able to view by default (comma separated list of Website IDs).

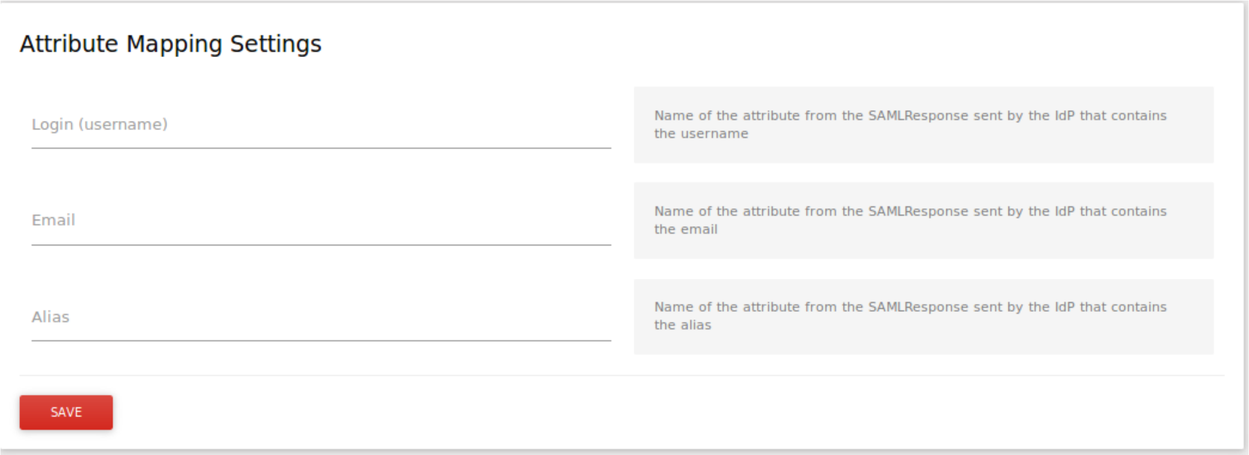
In order to identify your Matomo user accounts you need to set a value on the Field to identify the user, by default the email field will be used, but you can select username and the Matomo username field will be used.

You may also enable or disable the single logout functionality. Note that if you disable it, the Single Logout Service data will not be published on the Service Provider metadata.

You can also force users to use SAML authentication by enabling the “Force SAML Login” setting. Doing this will redirect all users directly to the Identity Provider, so the Matomo login screen will never be displayed. Super Users will still have to login normally to, for example, configure the SAML plugin. Super Users can login through the Matomo login screen by appending ?normal to the URL when visiting Matomo. (Note: other users will not be able to login this way.)

Attribute Mapping Settings

Depending on the values of Field to identify the user and just-in-time provisioning, the fields of the Attribute Mapping Settings section will be either required or optional.



Attribute Mapping Settings

Login (username)

Name of the attribute from the SAMLResponse sent by the IdP that contains the username

Email

Name of the attribute from the SAMLResponse sent by the IdP that contains the email

Alias

Name of the attribute from the SAMLResponse sent by the IdP that contains the alias

- If just-in-time is enabled, all mapping fields will be required.
- If just-in-time provisioning is disabled then only the field related to the value of Field to identify the user will be required.

Identity Providers sends to the Service Provider the user data with custom attribute names, so you can use the previous form to map names between IdP and Matomo.

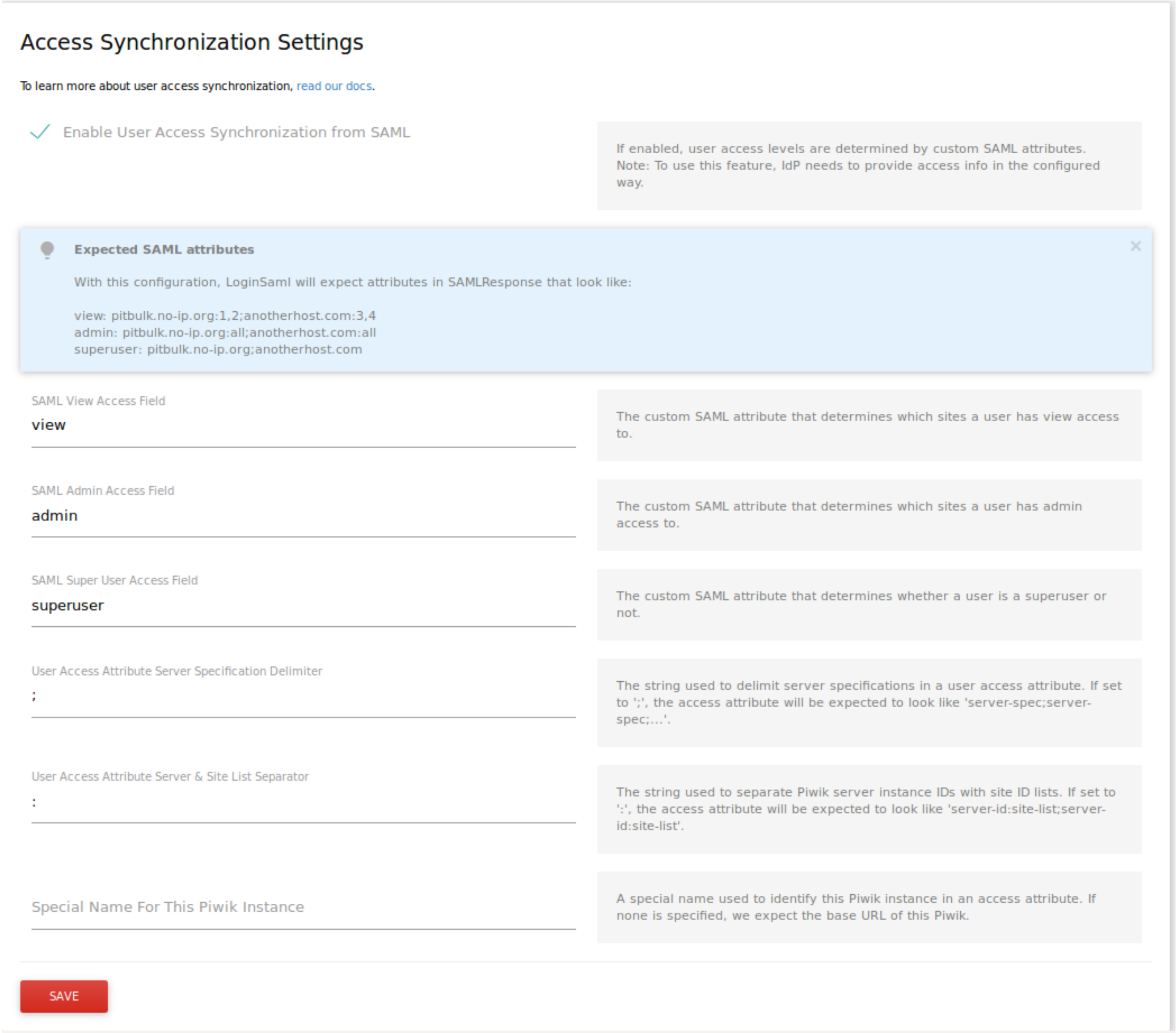
Access Synchronization settings

In the Access Synchronization settings section you can enable the user access synchronization from SAML attributes.

LoginSAML supports synchronizing access levels using attributes found in the SAMLResponse provided by the Identity provider. To use this feature, be sure that the IdP is providing access data in 3 different SAML attributes:

- an attribute to specify the sites a user has view access to (What is the view permission?)
- an attribute to specify the sites a user has admin access to (What is the admin permission?)
- and an attribute used to specify if a user is a superuser or not (What is the Super User in Matomo?)

Note: You can choose whatever names you want for these attributes. You will then tell LoginSaml about these names in the SAML settings page.



Access Synchronization Settings

To learn more about user access synchronization, read our docs.

✓ Enable User Access Synchronization from SAML

If enabled, user access levels are determined by custom SAML attributes. Note: To use this feature, IdP needs to provide access info in the configured way.

Expected SAML attributes

With this configuration, LoginSaml will expect attributes in SAMLResponse that look like:

```
view: pitbulk.no-ip.org:1,2;anotherhost.com:3,4
admin: pitbulk.no-ip.org:all;anotherhost.com:all
superuser: pitbulk.no-ip.org;anotherhost.com
```

SAML View Access Field: view

The custom SAML attribute that determines which sites a user has view access to.

SAML Admin Access Field: admin

The custom SAML attribute that determines which sites a user has admin access to.

SAML Super User Access Field: superuser

The custom SAML attribute that determines whether a user is a superuser or not.

User Access Attribute Server Specification Delimiter: ;

The string used to delimit server specifications in a user access attribute. If set to ';', the access attribute will be expected to look like 'server-spec;server-spec;...'.

User Access Attribute Server & Site List Separator: :

The string used to separate Piwik server instance IDs with site ID lists. If set to ':', the access attribute will be expected to look like 'server-id:site-list;server-id:site-list'.

Special Name For This Piwik Instance

A special name used to identify this Piwik instance in an access attribute. If none is specified, we expect the base URL of this Piwik.

Then in the SAML settings page, check the Enable User Access Synchronization from SAML checkbox and fill out the settings that appear below it.

User access synchronization occurs before the user logs in.

Identity provider access data example:

```
<saml:Attribute Name="view"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">all</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="admin"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">1,2,3</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="superuser"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">1</saml:AttributeValue>
</saml:Attribute>
```

Managing Access for Multiple Matomo Instances

LoginSaml supports using a single IdP SAML server to manage access for multiple Matomo instances. If you’d like to use this feature, you must specify special values for SAML access attributes. For example:

- view: mypiwikserver.whatever.com:1,2,3;myotherserver.com:all
- admin: mypiwikserver.whatever.com:all;mythirdserver.com:3,4
- superuser: myotherserver.com;myotherserver.com/otherpiwik

If you don’t want to use URLs in your access attributes, you can use the Special Name For This Matomo Instance setting to specify a special name for each of your Matomo instances. For example, if you set it to piwikServerA in one Matomo and piwikServerB in another, your SAML attributes might look like:

- view: piwikServerA:1,2,3;piwikServerB:all
- admin: piwikServerA:4,5,6
- superuser: piwikServerC

Using a custom access attribute format

You can customize the separators used in access attributes by setting the User Access Attribute Server Specification Delimiter and User Access Attribute Server & Site List Separator settings.

If you set the User Access Attribute Server Specification Delimiter option to #, access attributes can be specified as:

- view: piwikServerA:1,2,3#piwikServerB:all

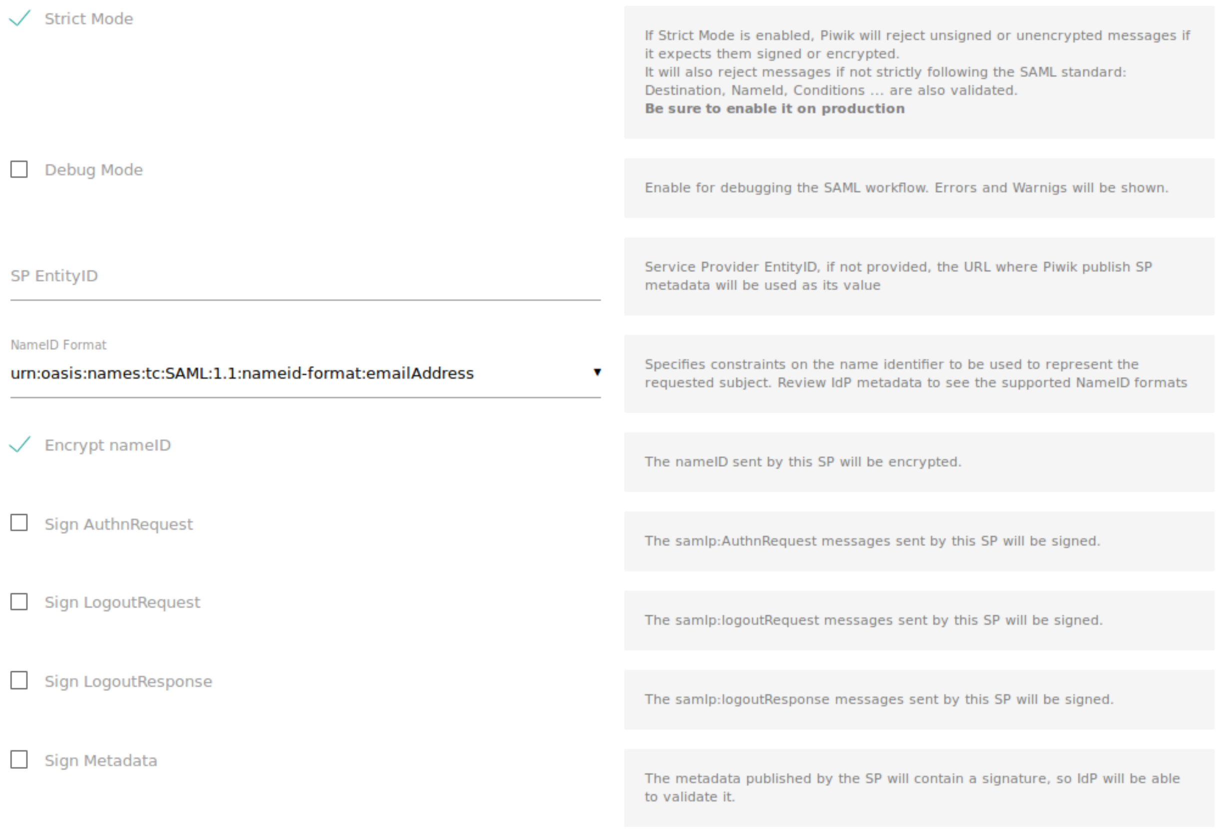
If you set the User Access Attribute Server & Site List Separator option to #, access attributes can be specified as:

- view: piwikServerA#1,2,3;piwikServerB#all

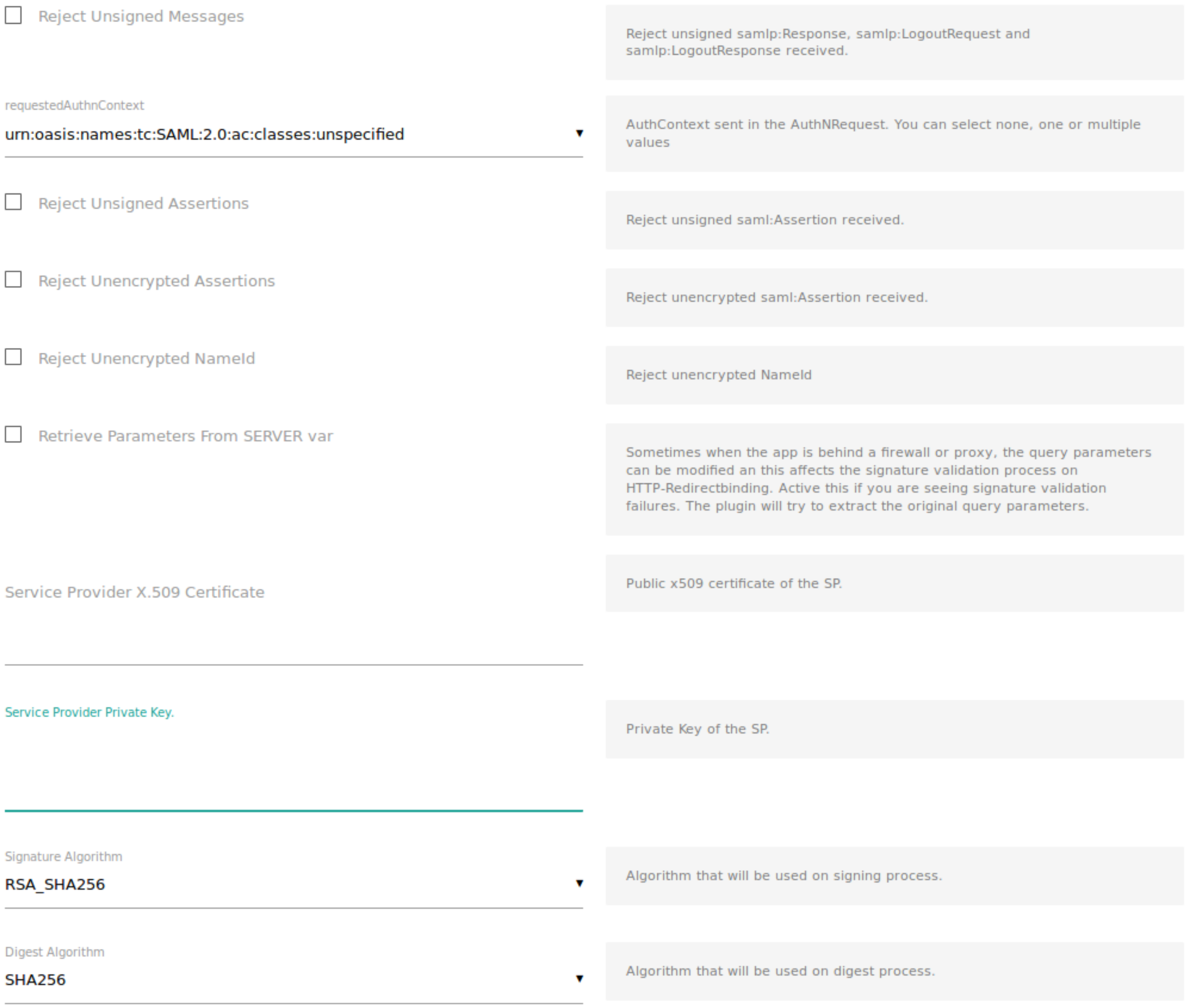
Advanced Settings

In the Advanced Settings section you can enable/disable the debug mode and also configure advanced SAML and security parameters.

Those settings match php-saml settings (the underlying PHP library in use in the SAML plugin and provided by OneLogin inc.), so you can review its documentation for more information.



✓ Strict Mode	If Strict Mode is enabled, Piwik will reject unsigned or unencrypted messages if it expects them signed or encrypted. It will also reject messages if not strictly following the SAML standard: Destination, NameId, Conditions ... are also validated. **Be sure to enable it on production**
□ Debug Mode	Enable for debugging the SAML workflow. Errors and Warnigs will be shown.
SP EntityID	Service Provider EntityID, if not provided, the URL where Piwik publish SP metadata will be used as its value
NameID Format urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ▾	Specifies constraints on the name identifier to be used to represent the requested subject. Review IdP metadata to see the supported NameID formats
✓ Encrypt nameID	The nameID sent by this SP will be encrypted.
□ Sign AuthnRequest	The samlp:AuthnRequest messages sent by this SP will be signed.
□ Sign LogoutRequest	The samlp:logoutRequest messages sent by this SP will be signed.
□ Sign LogoutResponse	The samlp:logoutResponse messages sent by this SP will be signed.
□ Sign Metadata	The metadata published by the SP will contain a signature, so IdP will be able to validate it.



☐ Reject Unsigned Messages

Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received.

requestedAuthnContext
urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified ▾

AuthContext sent in the AuthNRequest. You can select none, one or multiple values

☐ Reject Unsigned Assertions

Reject unsigned saml:Assertion received.

☐ Reject Unencrypted Assertions

Reject unencrypted saml:Assertion received.

☐ Reject Unencrypted NameId

Reject unencrypted NameId

☐ Retrieve Parameters From SERVER var

Sometimes when the app is behind a firewall or proxy, the query parameters can be modified an this affects the signature validation process on HTTP-Redirectbinding. Active this if you are seeing signature validation failures. The plugin will try to extract the original query parameters.

Service Provider X.509 Certificate

Public x509 certificate of the SP.

Service Provider Private Key.

Private Key of the SP.

Signature Algorithm
RSA_SHA256 ▾

Algorithm that will be used on signing process.

Digest Algorithm
SHA256 ▾

Algorithm that will be used on digest process.

Debugging

LoginSAML uses debug logging extensively so problems can be diagnosed quickly. Some logs entries contain sensitive information, so be sure to disable DEBUG logging in production and also switch off the Debug Mode in the Advanced Settings section of the SAML settings panel.

By default logs related with SAML will be found in Matomo folder tmp/logs/saml.log but can be changed defining a new value for the *logger_file_path* setting in the *[LoginSaml]* section of *config/config.ini.php*

The log level can be configured with the 'log_level' parameter and possible values are:

- ERROR
- WARN
- INFO
- DEBUG

The higher level, the smaller the number of entries in logs. The highest level is ERROR level (the lowest is DEBUG).

If no log_level parameter is defined in [LoginSaml] section then the default Matomo log_level value will be used (WARN).

FAQ

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.

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 Matomo page and not logged in?

There are some possible reasons for not be logged in:

- The IdP returned a SAMLResponse with status different from 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 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 side 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 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 Format's supported by the IdP (that is exposed in the IdP SAML metadata sometimes). If you are not sure what to set, configure it as unspecified, otherwise, emailAddress used to be the most common value.

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

No, you MUST enable it always in production environments.

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.

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

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

I'm using ADFS and when the Matomo SAML extension send the AuthNRequest I experience an error on ADFS side

There are many possible issues that 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.

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

Contact support 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 <matomo-folder>plugins/LoginSaml/vendor/onelogin/php-saml/certs

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

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

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 any research 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 just provided in new releases available on the marketplace.

Using Just-in-time provisioning and getting message “Username was not provided by the IdP and is required in order to execute the SAML Just-in-time provisioning”

The problem is that the Service Provider (Matomo) is not able to extract a username value from the SAMLResponse sent by the IdP. There are 2 possible reasons:

- The Attribute Mapping section at the SAML Settings of Matomo is wrong. There you might need to set the username field to the exact name of the attribute that came with the SAMLResponse.
- The IdP is not sending the username at all, so you may need to contact the Identity Provider administrator and ask him to configure the IdP to provide that user info.

Note that even if you are identifying users by the email address, the username is a required field when you are using Just-in-time provisioning: so both email and username must be provided. You can find out more about your SAML response by using the SAML Tracer tool.

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.