

Overview

[Tiki17](#) and later can be a SAML Service Provider (SP), thanks to the integration of [OneLogin's SAML PHP Toolkit](#).

Up to [Tiki23](#), it requires installation via [Packages](#). Starting in [Tiki24](#), it is built-in.

When setting up Tiki as a SAML Service Provider, you would need to provide to the IdP the URLs for assertion consumer service, and single logout service (if used). These are : `http<your site baseurl>/tiki-login.php?saml_acs` and `http<your site baseurl>/tiki-login.php?saml_sls` respectively.

Option	Description	Default
Enable SAML Auth		Disabled
IdP Entity Id	Identifier of the IdP entity ("Issuer")	<input type="text"/>
Single sign-on service URL	SSO endpoint info of the IdP, the URL target of the IdP where the SP will send the Authentication Request ("SAML 2.0 Endpoint (HTTP)")	<input type="text"/>
Single log-out service URL	SLO endpoint info of the IdP, the URL target of the IdP where the SP will send the SLO Request ("SLO Endpoint (HTTP)")	<input type="text"/>
X.509 certificate	Public x509 certificate of the IdP. ("X.509 certificate")	<input type="text"/>
Create user if not registered in Tiki	Auto-provisioning - if the user doesn't exist, Tiki will create a new user with the data provided by the IdP. Review the Mapping section.	<input type="checkbox"/>
Sync user group with IdP data	This should be enabled to sync groups with the IdP.	<input type="checkbox"/>
Enable Single Logout Service	The "logout" function logs out the user from the Tiki site, the identity provider and all connected service providers	<input type="checkbox"/>
Use Tiki authentication for Admin log-in	The user "admin" will be authenticated by only using Tiki's user database. This option has no effect on users other than "admin".	Enabled
Account matcher	Select the field to be used to find the user account. If the "email" field is selected, keep in mind that if users change their email address, then the link with the IdP account will be lost. <input type="checkbox"/> Username <input type="checkbox"/> Email	Email
Default group	When provisioning a new user and not group found, assign that group	Registered

Option	Description	Default
Log-in link text	The text that appears on the log-in page	Log in through SAML2 IdP
SAML attribute that will be mapped to the Tiki username	The SAML attribute that will be mapped to the Tiki username.	<input type="text"/>
SAML attribute that will be mapped to the Tiki email	The SAML attribute that will be mapped to the Tiki email.	<input type="text"/>
SAML attribute that will be mapped to the Tiki group	The SAML attribute that will be mapped to the Tiki email. For example the eduPersonAffiliation	<input type="text"/>
Admins	Set here the values of the IdP related to the user group info that will be matched with the Admins group.	<input type="text"/>
Registered	Set here the values of the IdP related to the user group info that will be matched with the Registered group.	<input type="text"/>
Debug Mode	Enable debug mode when your are debugging the SAML workflow. Errors and warnings will be showed..	<input type="text"/>
Strict Mode	Always enable strict mode on production websites. When strict mode is enabled, then Tiki will reject unsigned or unencrypted messages if it expects them to be signed or encrypted. Also Tiki will reject messages that do not strictly follow the SAML standard: Destination, NameId, Conditions . . . are also validated.	<input type="text"/>
Service Provider Entity ID	Set the Entity ID for the service provider. It is recommended to set as the SP Entity ID the URL where the metadata of the service provider is published. If not provided, the toolkit will use "php-saml" as the SP entityID.	<input type="text"/>
Requested NameIDFormat	Specifies constraints on the name identifier to be used to represent the requested subject. ☰ urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName urn:oasis:names:tc:SAML:2.0:nameid-format:entity urn:oasis:names:tc:SAML:2.0:nameid-format:transient urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted urn:oasis:...	urn:oasis:names:tc:SAML:1.1...

Option	Description	Default
Requested AuthnContext	Authentication context: unselect all to accept any type, otherwise select the valid contexts. ☰ urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified urn:oasis:names:tc:SAML:2.0:ac:classes:Password urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport urn:oasis:names:tc:SAML:2.0:ac:classes:X509 urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos urn:federation:authentication:windows	urn:oasis:names:tc:SAML:2.0...
Encrypt nameID		☐☐☐☐
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 this SP will be signed	☐☐☐☐
Reject Unsigned Messages	Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received	☐☐☐☐
Reject Unsigned Assertions	Reject unsigned saml:Assertion received	☐☐☐☐
Reject Unencrypted Assertions	Reject unencrypted saml:Assertion received	☐☐☐☐
Retrieve Parameters From Server	Sometimes when the app is behind a firewall or proxy, the query parameters can be modified and this affects the signature validation process on HTTP-Redirect binding. Active this when you noticed 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	Algorithm that the toolkit will use on the signing process ☰ http://www.w3.org/2000/09/xmldsig#rsa-sha1 http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 http://www.w3.org/2000/09/xmldsig#dsa-sha1	http://www.w3.org/2000/09/x...

Option	Description	Default
Enable Lowercase URL encoding	Some IdPs such as ADFS can use lowercase URL encoding, but the plugin expects uppercase URL encoding, so enable it to fix incompatibility issues..	<input type="checkbox"/>

Option	Description	Default
Enable SAML Auth		Disabled
IdP Entity Id	Identifier of the IdP entity ("Issuer")	<input type="text"/>
Single sign-on service URL	SSO endpoint info of the IdP, the URL target of the IdP where the SP will send the Authentication Request ("SAML 2.0 Endpoint (HTTP)")	<input type="text"/>
Single log-out service URL	SLO endpoint info of the IdP, the URL target of the IdP where the SP will send the SLO Request ("SLO Endpoint (HTTP)")	<input type="text"/>
X.509 certificate	Public x509 certificate of the IdP. ("X.509 certificate")	<input type="text"/>
Create user if not registered in Tiki	Auto-provisioning - if the user doesn't exist, Tiki will create a new user with the data provided by the IdP. Review the Mapping section.	<input type="checkbox"/>
Sync user group with IdP data	This should be enabled to sync groups with the IdP.	<input type="checkbox"/>
Enable Single Logout Service	The "logout" function logs out the user from the Tiki site, the identity provider and all connected service providers	<input type="checkbox"/>
Use Tiki authentication for Admin log-in	The user "admin" will be authenticated by only using Tiki's user database. This option has no effect on users other than "admin".	Enabled
Account matcher	Select the field to be used to find the user account. If the "email" field is selected, keep in mind that if users change their email address, then the link with the IdP account will be lost. ☰ Username Email	Email
Default group	When provisioning a new user and not group found, assign that group	Registered
Log-in link text	The text that appears on the log-in page	Log in through SAML2 IdP
SAML attribute that will be mapped to the Tiki username	The SAML attribute that will be mapped to the Tiki username.	<input type="text"/>

Option	Description	Default
Sign LogoutRequest	The samlp:logoutRequest messages sent by this SP will be signed	<input type="checkbox"/>
Sign LogoutResponse	The samlp:logoutResponse messages sent by this SP will be signed	<input type="checkbox"/>
Sign Metadata	The Metadata published by this SP will be signed	<input type="checkbox"/>
Reject Unsigned Messages	Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received	<input type="checkbox"/>
Reject Unsigned Assertions	Reject unsigned saml:Assertion received	<input type="checkbox"/>
Reject Unencrypted Assertions	Reject unencrypted saml:Assertion received	<input type="checkbox"/>
Retrieve Parameters From Server	Sometimes when the app is behind a firewall or proxy, the query parameters can be modified and this affects the signature validation process on HTTP-Redirect binding. Active this when you noticed signature validation failures, the plugin will try to extract the original query parameters.	<input type="checkbox"/>
Service Provider X.509 certificate	Public x509 certificate of the SP	<input type="checkbox"/>
Service Provider Private Key	Private key of the SP	<input type="checkbox"/>
Signature Algorithm	Algorithm that the toolkit will use on the signing process ⌵ http://www.w3.org/2000/09/xmlsig#rsa-sha1 http://www.w3.org/2001/04/xmlsig-more#rsa-sha256 http://www.w3.org/2001/04/xmlsig-more#rsa-sha384 http://www.w3.org/2001/04/xmlsig-more#rsa-sha512 http://www.w3.org/2000/09/xmlsig#dsa-sha1	http://www.w3.org/2000/09/x...
Enable Lowercase URL encoding	Some IdPs such as ADFS can use lowercase URL encoding, but the plugin expects uppercase URL encoding, so enable it to fix incompatibility issues..	<input type="checkbox"/>

Option	Description	Default
Enable SAML Auth		Disabled
IdP Entity Id	Identifier of the IdP entity ("Issuer")	<input type="checkbox"/>
Single sign-on service URL	SSO endpoint info of the IdP, the URL target of the IdP where the SP will send the Authentication Request ("SAML 2.0 Endpoint (HTTP)")	<input type="checkbox"/>

Option	Description	Default
Single log-out service URL	SLO endpoint info of the IdP, the URL target of the IdP where the SP will send the SLO Request ("SLO Endpoint (HTTP)")	<input type="text"/>
X.509 certificate	Public x509 certificate of the IdP. ("X.509 certificate")	<input type="text"/>
Create user if not registered in Tiki	Auto-provisioning - if the user doesn't exist, Tiki will create a new user with the data provided by the IdP. Review the Mapping section.	<input type="checkbox"/>
Sync user group with IdP data	This should be enabled to sync groups with the IdP.	<input type="checkbox"/>
Enable Single Logout Service	The "logout" function logs out the user from the Tiki site, the identity provider and all connected service providers	<input type="checkbox"/>
Use Tiki authentication for Admin log-in	The user "admin" will be authenticated by only using Tiki's user database. This option has no effect on users other than "admin".	Enabled
Account matcher	Select the field to be used to find the user account. If the "email" field is selected, keep in mind that if users change their email address, then the link with the IdP account will be lost. ☰ Username Email	Email
Default group	When provisioning a new user and not group found, assign that group	Registered
Log-in link text	The text that appears on the log-in page	Log in through SAML2 IdP
SAML attribute that will be mapped to the Tiki username	The SAML attribute that will be mapped to the Tiki username.	<input type="text"/>
SAML attribute that will be mapped to the Tiki email	The SAML attribute that will be mapped to the Tiki email.	<input type="text"/>
SAML attribute that will be mapped to the Tiki group	The SAML attribute that will be mapped to the Tiki email. For example the eduPersonAffiliation	<input type="text"/>
Admins	Set here the values of the IdP related to the user group info that will be matched with the Admins group.	<input type="text"/>
Registered	Set here the values of the IdP related to the user group info that will be matched with the Registered group.	<input type="text"/>
Debug Mode	Enable debug mode when your are debugging the SAML workflow. Errors and warnings will be showed..	<input type="checkbox"/>

Option	Description	Default
Strict Mode	Always enable strict mode on production websites. When strict mode is enabled, then Tiki will reject unsigned or unencrypted messages if it expects them to be signed or encrypted. Also Tiki will reject messages that do not strictly follow the SAML standard: Destination, NameId, Conditions . . . are also validated.	<input type="checkbox"/>
Service Provider Entity ID	Set the Entity ID for the service provider. It is recommended to set as the SP Entity ID the URL where the metadata of the service provider is published. If not provided, the toolkit will use "php-saml" as the SP entityID.	<input type="checkbox"/>
Requested NameIDFormat	Specifies constraints on the name identifier to be used to represent the requested subject. <div> <input type="checkbox"/> urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified <input type="checkbox"/> urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress <input type="checkbox"/> urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:nameid-format:entity <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:nameid-format:transient <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:nameid-format:persistent <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted urn:oasis:... </div>	urn:oasis:names:tc:SAML:1.1...
Requested AuthnContext	Authentication context: unselect all to accept any type, otherwise select the valid contexts. <div> <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:Password <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:X509 <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard <input type="checkbox"/> urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos <input type="checkbox"/> urn:federation:authentication:windows </div>	urn:oasis:names:tc:SAML:2.0...
Encrypt nameID		<input type="checkbox"/>
Sign AuthnRequest	The samlp:AuthnRequest messages sent by this SP will be signed	<input type="checkbox"/>
Sign LogoutRequest	The samlp:logoutRequest messages sent by this SP will be signed	<input type="checkbox"/>
Sign LogoutResponse	The samlp:logoutResponse messages sent by this SP will be signed	<input type="checkbox"/>
Sign Metadata	The Metadata published by this SP will be signed	<input type="checkbox"/>
Reject Unsigned Messages	Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received	<input type="checkbox"/>
Reject Unsigned Assertions	Reject unsigned saml:Assertion received	<input type="checkbox"/>
Reject Unencrypted Assertions	Reject unencrypted saml:Assertion received	<input type="checkbox"/>

Option	Description	Default
Retrieve Parameters From Server	Sometimes when the app is behind a firewall or proxy, the query parameters can be modified and this affects the signature validation process on HTTP-Redirect binding. Active this when you noticed signature validation failures, the plugin will try to extract the original query parameters.	<input type="checkbox"/>
Service Provider X.509 certificate	Public x509 certificate of the SP	<input type="text"/>
Service Provider Private Key	Private key of the SP	<input type="text"/>
Signature Algorithm	Algorithm that the toolkit will use on the signing process ⌵ http://www.w3.org/2000/09/xmldsig#rsa-sha1 http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 http://www.w3.org/2000/09/xmldsig#dsa-sha1	http://www.w3.org/2000/09/x...
Enable Lowercase URL encoding	Some IdPs such as ADFS can use lowercase URL encoding, but the plugin expects uppercase URL encoding, so enable it to fix incompatibility issues..	<input type="checkbox"/>

Wikipedia wrote:

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The single most important requirement that SAML addresses is web browser single sign-on (SSO). Single sign-on is common at the intranet level (using cookies, for example) but extending it beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. (Another more recent approach to addressing the browser SSO problem is the OpenID Connect protocol.)

Source: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Related links

- See also [Tiki as a SAML IDP](#)
- https://en.wikipedia.org/wiki/Identity_provider
- https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language