Log-in - General preferences

Option	Description	Default
Authentication method	Tiki supports several authentication methods. The default method is to use the internal user database. ≣ Tiki | Tiki and OpenID Connect | Tiki and PAM | Tiki and LDAP | CAS (Central Authentication Service) | Shibboleth | Web Server | phpBB	Tiki
Intertiki	Allows several Tiki sites (slaves) to get authentication from a master Tiki site	Disabled
User must change password set default on	Set default value for the 'user must change password at next login' checkbox in the registration form when adding new user by the admin. This is to avoid to have to check the said checkbox everytime on next user's creation if your policy is that the new user must change the password given by the admin at next login.	Disabled
Users can register	Allow site visitors to register, using the registration form. The log-in module will include a "Register" link. If this is not activated, new users will have to be added manually by the admin on the Admin-Users page.	Disabled
Validate new user registrations by email	Tiki will send an email message to the user. The message contains a link that must be clicked to validate the registration. After clicking the link, the user will be validated. You can use this option to limit false registrations or fake email addresses.	Enabled
Validate user's email server	Tiki will attempt to validate the user's email address by examining the syntax of the email address. It must be a string of letters, or digits or _ or . or - follows by a @ follows by a string of letters, or digits or _ or . or -. Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server. ≣ No | Yes | Yes, with "deep MX" search	No
Require validation by Admin	The administrator will receive an email for each new user registration, and must validate the user before the user can log in.	Disabled
Validator emails (separated by comma) if different than the sender email		None
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled
Passcode	👆 *Alphanumeric code required to complete the registration*	None

Option	Description	Default
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue 👆 *Key required to be on included the URL to access the registration page (if not empty).*	None
Generate password	Display a button on the registration form to automatically generate a very secure password for the user. 👆 *The generated password may not include any restrictions (such as minimum/maximum length.*	Disabled
Registration referrer check	Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)	Enabled
Display Disposable Emails	Show if a user's email address is from a disposable / temporary email address provider	Disabled
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display. ☰ 2 | 4 | 6 | 8 | 10	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. 👆 *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA 👆 *You will need to register at http://www.google.com/recaptcha*	Disabled
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. ☰ Clean | Black Glass | Red | White	Clean
Version	reCAPTCHA version. ☰ 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line 👆 *One question per line with a colon separating the question and answer*	None

Option	Description	Default
Users must choose a group at registration	Users cannot register without choosing one of the groups indicated above.	Disabled
URL the user is redirected to after account validation	The default page a Registered user sees after account validation is "tiki-information.php?msg=Account validated successfully". 👆 *Default: tiki-information.php?msg=Account validated successfully.*	None
Use a tracker to collect more user information	Display a tracker form for the user to complete as part of the registration process. This tracker will receive and store additional information about each user. 👆 *Go to Admin Groups to select which tracker and fields to display.*	Disabled
Add a user tracker item for new user set default on	Set default value for the "add a user tracker item for this user" checkbox in the registration form when adding new user by the admin. This is to avoid to have to check the said checkbox everytime on next users creation if your policy is that you want to add a tracker item in the user tracker when creating a new user.	Disabled
Present different input fields in the User Wizard than are in the Registration form	Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form	Disabled
Tracker fields presented in the User Wizard as User Details	User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)	None
Use pretty trackers for registration form	Allows a site manager to design forms using registration fields and have the results of each field displayed in customizable way on a Wiki page or Smarty template.	Disabled
Registration pretty tracker template	Use a wiki page name or Smarty template file with a .tpl extension.	None
Hide Mandatory	Hide mandatory fields indication with an asterisk (shown by default).	Disabled
Output the registration results	Use a wiki page as template to output the registration results to	Disabled
Output registration pretty tracker template	Wiki page only	None
Page name field ID	Use the tracker's field ID whose value is used as the output page name.	None
User tracker IDs to sync prefs from	Select one or more trackers to sync user preferences from.	None
Tracker field IDs to sync the "real name" pref from	Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using "+", for example "2+3,4".	None
Tracker field IDs to sync user groups	Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.	None

Option	Description	Default
Synchronize long/lat/zoom to location field	Synchronize user geolocation preferences with the main location field.	Disabled
Change user system language when changing user tracker item language		Disabled
Assign a user tracker item when registering if email equals this field		None
Force users to upload an avatar.	Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.	Disabled
Require users to fill in tracker information	Require users to fill in a tracker form if not done already by prompting them with a modal dialog.	Disabled
Tracker ID of tracker required to be filled in	A tracker for articles must contain an "Articles" field	None
Mandatory tracker field to check for required filling in	The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.	None
Fields that are asked for in the modal for force-filling	Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested	None
Use tracker to collect more group information	👆 *Go to Admin Groups to select which tracker and fields to display.*	Disabled
Re-validate user email after	The number of days after which an email will be sent to the user with a link to revalidate the account. The user will not be able to login (that is, the account will be invalid), until the user clicks the link. Use this feature to verify that a user's email is still valid. 👆 *Use "-1" for never*	-1 days
Re-validate user by email after	After a certain number of consecutive unsuccessful log-in attempts, the user will receive an email with instruction to validate his or her account. However, the user can still log in with the old password. 👆 *Use "-1" for never*	20 unsuccessful login attempts
Suspend/lockout account after	After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin must revalidate the account before the user can use it again. 👆 *Use "-1" for never*	50 unsuccessful login attempts

Option	Description	Default
Create a new group for each user	Automatically create a group for each user in order to, for example, assign permissions on the individual-user level. 👆 *The group name will be the same as the user's username*	Disabled
Disable browser's autocomplete feature for username and password fields	Use to deactivate the autocomplete in the log-in box. The autocomplete features can be optionally set in the user's browser to remember the form input and proposes the remember the password. If enabled, the user log-in name and password cannot be remembered. You should enable this feature for highly secure sites.	Disabled
Enable placeholders feature for username and password fields	Show placeholder text from username and password fields in the login form. Enable this if you want to show the placeholder text.	Disabled
On permission denied, display login module	If an anonymous visitor attempts to access a page for which permission is not granted, Tiki will automatically display the Log-in module. Alternatively, use the Send to URL field to display a specific page (relative to your Tiki installation) instead.	Enabled
Descriptive sentence to ask a user to log in	If the login module is called on the page and shown to users who are not logged in, this sentence may ask them to enter their credentials (supports wiki syntax)	None
Prevent multiple log-ins by the same user	Users (other than admin) cannot log in simultaneously with multiple browsers.	Disabled
Clean expired cookies	Automatically clean expired cookies from the database when anyone logs in.	Enabled
Grab session if already logged in	If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out	Disabled
Protect all sessions with HTTPS	Always redirect to HTTPS to prevent a session hijack through network sniffing. ⚠ *Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site*	Disabled
Use HTTPS login	Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server. ⚠ *Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible* ☰ Disabled | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login	Allow secure (HTTPS) login
HTTP Basic Authentication	Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials. ☰ Disable | SSL Only (Recommended) | Always	Disable

Option	Description	Default
Users can choose to stay in SSL mode after an HTTPS login		Disabled
Users can switch between secured or standard mode at login		Disabled
HTTP port	The port used to access this server; if not specified, port %0 will be used 👆 *If not specified, port %0 will be used*	None
HTTPS port	the HTTPS port for this server.	443
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled
Remember me	After logging in, users will automatically be logged in again when they leave and return to the site. ☰ Disabled | User's choice | Always	User's choice
Duration	The length of time before the user will need to log in again. ☰ 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 8 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year	1 month
Refresh the remember-me cookie expiration	Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.	Enabled
Cookie name	Name of the cookie to remember the user's login 👆 *Changing the cookie name forces an instant logout for all user sessions. Including yours.*	Tikiwiki
Domain	The domain that the cookie is available to.	None
Path	The path on the server in which the cookie will be available on. Tiki will detect if it is installed in a subdirectory and will use that automatically. 👆 *N.B. Needs to start with a / character to work properly in Safari*	/
Cookie Consent	Ask permission of the user before setting any cookies, and comply with the response. 👆 *Complies with EU Privacy and Electronic Communications Regulations.* ⚗	Disabled
Cookie consent name	Name of the cookie to record the user's consent if the user agrees. ⚗	Tiki_cookies_accepted
Cookie consent expiration	Expiration date of the cookie to record consent (in days). ⚗	365 days
Cookie consent text	Description for the dialog. 👆 *Wiki-parsed* ⚗	privacy notice.">This website would like to ...

Option	Description	Default
Cookie consent question	Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. 👆 *Wiki-parsed* ⚗	I accept cookies from this ...
Cookie consent for analytics	Make it possible for users to opt in to essential cookies, such as "remember login", "timezone" etc without opting in to third party cookies such as those for Google Analytics and other external services. 👆 *Makes the checkbox opt in to accept "non-essential" cookies* ⚗	Disabled
Cookie consent alert	Alert displayed when user tries to access or use a feature requiring cookies. ⚗	Sorry, cookie consent required
Cookie consent button	Label on the agreement button. ⚗	Continue
Cookie consent display mode	Appearance of consent dialog ☰ Plain | Banner | Dialog ⚗	None
Cookie consent dialog ID	DOM id for the dialog container div. ⚗	Cookie_consent_div
Cookie consent disabled	Do not give the option to refuse cookies but still inform the user about cookie usage. ⚗	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Ban usernames and emails	Banning rules use both email and username to match rules.	Disabled
Attempts number	Number of attempts user is allowed to login incorrectly before banning them from further attempts.	5
Banning system	The duration of the incorrect login attempts ban in minutes.	30
Use email as username	Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.	Disabled
Obscure email when using email as username	This will attempt as much as possible to hide the email address, showing the real name or the truncated email address instead. ⚠ *Coverage will not be complete*	Disabled
User emails must be unique	The email address of each user must be unique.	Disabled
Show emails validation	Show if an email is already in use on the registration form. Will confirm an email is registered here if so without completing the form.	Enabled
User can login via username or email.	This will allow users to login using their email (as well as their username).	Disabled
Minimum length	The least possible number of characters for a valid username.	1 characters
Maximum length	The greatest number of characters for a valid username.	50 characters

Option	Description	Default
Force lowercase	Automatically convert all alphabetic characters in the username to lowercase letters. For example **JohnDoe** becomes **johndoe**.	Disabled
Username pattern	This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /'\-_a-zA-Z0-9@\.א-ת*$/ or, for Chinese, use: /'\-_a-zA-Z0-9@\.\x00-\xff*$/	/^'\-_a-zA-Z0-9@\.*$/
Auto-generate 6-digit username on registration	This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).	Disabled
Forgot password	Users can request a password reset. They will receive a link by email. ✳ *Since passwords are stored securely, it's not possible to tell the user what the password is. It's only possible to change it.*	Enabled
Allow users to use 2FA	Allow users to enable Two-factor Authentication.	Disabled
Force all users to use 2FA	This will force all users to activate 2FA.	Disabled
Force users in the indicated groups to enable 2FA	List of group names.	None
Force indicated users to enable 2FA	List of usernames.	None
Do not force users in the indicated groups to enable 2FA	List of group names.	None
Do not force indicated users to enable 2FA	List of usernames.	None
Users can change their password	Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.	Enabled
Require characters and numerals	For improved security, require users to include a mix of alphabetical characters and numerals in passwords.	Disabled
Require alphabetical characters in lower and upper case	Password must contain at least one lowercase alphabetical character like "a" and one uppercase character like "A". Use this option to require users to select stronger passwords.	Disabled
Require special characters	Password must contain at least one special character in lower case like **" / $ % ? & * ( ) _ + .** Use this option to require users to select stronger passwords.	Disabled

Option	Description	Default
Require no consecutive repetition of the same character	Password must not contain a consecutive repetition of the same character such as "111" or "aab".	Disabled
Prevent common passwords	For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.	Disabled
The password must be different from the user's log-in name		Enabled
Minimum length	The least possible number of characters for a valid password.	5 characters
Password expires after	The number of days after which a password will expire. Days are counted starting with the user's first login. When the password expires, users will be required to select a new password when logging in. 👆 Use "-1" for never	-1 days
Password History Management	To enforce password security, this option allows to determine the number of password resets associated with a user account before the password can be reused.	Disabled
Use old password after	Number of password resets before the password can be reused.	5 resets

Log-in - CAS

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database.	Disabled
Try automatically to connect SSO		Disabled
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".	Disabled
Show alternate log-in method in header		Enabled
Force CAS log-out when the user logs out from Tiki.		Disabled
CAS server version	☰ none | Version 1.0 | Version 2.0	Version 1.0
Hostname	Hostname of the CAS server.	None
Port	Port of the CAS server.	443

Option	Description	Default
Path	Path for the CAS server.	None
CAS Extra Parameter	Extra Parameter to pass to the CAS Server.	None
CAS Authentication Verification Timeout	Verify authentication with the CAS server every N seconds. Null value means never reverify. ☰ Never | 1 minute | 2 minutes | 5 minutes | 10 minutes | 15 minutes | 30 minutes | 1 hour	0

Log-in - LDAP

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database. ⚠ *If this option is disabled, this user wouldn't be able to log in.* ☰ Create the user | Deny access	Create the user
Require admin validation for LDAP users	When externally authenticated user is created in Tiki database either allow immediate login or create in disabled state that requires an administrator to approve the account before user can login to Tiki.	Disabled
Create user if not in LDAP	If a user was authenticated by Tiki's user database, but not found on the LDAP server, Tiki will create an LDAP entry for this user. ⚠ *As of this writing, this is not yet implemented, and this option will probably not be offered in future.* ⚗	Disabled
Use Tiki authentication for Admin log-in	If this option is set, the user "admin" will be authenticated by only using Tiki's user database and not via LDAP. This option has no effect on users other than "admin".	Enabled
Use Tiki authentication for users created in Tiki	If this option is set, users that are created using Tiki are not authenticated via LDAP. This can be useful to let external users (ex.: partners or consultants) access Tiki, without being in your main user list in LDAP.	Disabled
Host	The hostnames, ip addresses or URIs of your LDAP servers. Separate multiple entries with Whitespace or ','. If you use URIs, then the settings for Port number and SSL are ignored. Example: "localhost ldaps://master.ldap.example.org:63636" will try to connect to localhost unencrypted and if if fails it will try the master LDAP server at a special port with SSL.	None
Port	The port number your LDAP server uses (389 is the default, 636 if you check SSL).	None

Option	Description	Default
Write LDAP debug information in Tiki Logs	Write debug information to Tiki logs (Admin -> Tiki Logs, Tiki Logs have to be enabled). ⚠️ *Do not enable this option for production sites.*	Disabled
Use SSL (ldaps)		Disabled
Use TLS		Disabled
LDAP Bind Type	• **Active Directory bind** will build a RDN like username at example.com where your basedn is (dc=example, dc=com) and username is your username • **Plain bind** will build a RDN username • **Full bind** will build a RDN like userattr=username, userdn, basedn where userattr is replaced with the value you put in 'User attribute', userdn with the value you put in 'User DN', basedn with the value with the value you put in 'base DN' • **OpenLDAP bind** will build a RDN like cn=username, basedn • **Anonymous bind** will build an empty RDN ☰ Default: Anonymous Bind | Full: userattr=username,UserDN,BaseDN | OpenLDAP: cn=username,BaseDN | Active Directory (username@domain) | Plain Username	Default: Anonymous Bind
Search scope	Used after authentication for getting user and group information. ☰ Subtree | One level | Base object	Subtree
Base DN		None
User DN		None
User attribute		Uid
User OC		InetOrgPerson
Realname attribute	Synchronize Tiki user attributes with the LDAP values.	DisplayName
Country attribute	Synchronize Tiki user attributes with the LDAP values.	None
Email attribute	Synchronize Tiki user attributes with the LDAP values.	None
Admin user		None
Admin password		None

Log-in - LDAP external groups

Option	Description	Default
Use an external LDAP server for groups		Disabled
Host		Localhost
Port		389
Write LDAP debug Information in Tiki Logs	Write debug information to Tiki logs (Admin -> Tiki Logs, Tiki Logs have to be enabled). ⚠️ *Do not enable this option for production sites.*	Disabled
Use SSL (ldaps)		Disabled
Use TLS		Disabled
LDAP Bind Type	• **Active Directory bind** will build a RDN like username at example.com where your basedn is (dc=example, dc=com) and username is your username • **Plain bind** will build a RDN username • **Full bind** will build a RDN like userattr=username, userdn, basedn where userattr is replaced with the value you put in 'User attribute', userdn with the value you put in 'User DN', basedn with the value with the value you put in 'base DN' • **OpenLDAP bind** will build a RDN like cn=username, basedn • **Anonymous bind** will build an empty RDN ☰ Anonymous Bind | Full: userattr=username,UserDN,BaseDN | OpenLDAP: cn=username,BaseDN | Active Directory (username@domain) | Plain Username	Anonymous Bind
Search scope	☰ Subtree | One level | Base object	Subtree
Base DN		None
User DN		None
User attribute		Uid
Corresponding user attribute in 1st directory		Uid
User OC		InetOrgPerson
Synchronize Tiki groups with a directory	👆 *Define the directory within the "LDAP" tab*	Disabled
Group DN		None

Option	Description	Default
Group name attribute		Cn
Group description attribute		None
Group OC		GroupOfUniqueNames
Synchronize Tiki users with a directory	👆 *Define the directory within the "LDAP" tab*	Disabled
Member attribute		UniqueMember
Member is DN		Enabled
Group attribute		None
Group attribute in group entry	👆 *(Leave this empty if the group name is already given in the user attribute)*	None
Admin user		None
Admin password		None

Log-in - PAM

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database.	Disabled
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".	Disabled

Log-in - Password Blacklist

Option	Description	Default
Password file used	The automatically selected file is recommended unless you generate your own blacklist file. ☰ Automatically select blacklist | Num & Let: 0, Special: 0, Min Len: 1, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 5, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 7, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 0, Min Len: 9, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 1, Min Len: 1, Custom: 0, Word Count: 1000 | Num & Let: 0, Special: 1...	Automatically select blacklist

Log-in - PHPBB

Option	Description	Default
Create user if not registered in Tiki	Automatically create a new Tiki user for the PHPbb login	Disabled
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". 👆 *Recommended*	Enabled
Disable Tiki users with no phpBB login	Disable Tiki users who don't have a phpBB login as they could have been deleted. 👆 *Recommended*	Disabled
phpBB Version	☰ 3	3
phpBB Database Hostname		None
phpBB Database Username		None
phpBB Database Password		None
phpBB Database Name		None
phpBB Table Prefix		Phpbb_

Log-in - Remote Tiki auto-login

Option	Description	Default
Enable autologin from remote Tiki	Used with autologin_remotetiki in the redirect plugin	Disabled
System username to use to initiate autologin from remote Tiki	Specified user must exist and be configured in Settings...Tools...DSN/Content Authentication on remote Tiki. Used with autologin_remotetiki in the redirect plugin.	None
System groupname to use for auto login token	For security, please create a group that has no users and no permissions and specify its name here.	None
Create user if not registered in Tiki	Create a new user account if the user that is trying to autologin does not exist on this Tiki.	Enabled
Allowed groups from remote Tiki to autologin.	Comma-separated list of groups to allow autologin from remote Tiki. If empty, will allow everyone.	None
Sync these groups from remote Tiki on autologin.	Comma-separated list of groups to sync from remote Tiki on autologin. Group membership will be added or removed accordingly.	None
Automatically logout remote Tiki after logout.	When the user logs out of this Tiki, redirect the user to logout of the other Tiki as well.	Enabled
Redirect direct logins to this site to remote Tiki	Redirect direct logins to this site to remote Tiki	Disabled
URL of autologin page on remote Tiki to redirect user to login	URL of autologin page on remote Tiki to redirect user to login, e.g. https://www.remotetiki.com/PageWithRedirectPlugin	None

Log-in - SAML2

Option	Description	Default
Enable SAML Auth		Disabled
IdP Entity Id	Identifier of the IdP entity ("Issuer")	None
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)")	None
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)")	None
X.509 certificate	Public x509 certificate of the IdP. ("X.509 certificate")	None
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.	None
Sync user group with IdP data	This should be enabled to sync groups with the IdP.	None
Enable Single Logout Service	The "logout" function logs out the user from the Tiki site, the identity provider and all connected service providers	None
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.	None
SAML attribute that will be mapped to the Tiki email	The SAML attribute that will be mapped to the Tiki email.	None

Option	Description	Default
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	None
Admins	Set here the values of the IdP related to the user group info that will be matched with the Admins group.	None
Registered	Set here the values of the IdP related to the user group info that will be matched with the Registered group.	None
Debug Mode	Enable debug mode when your are debugging the SAML workflow. Errors and warnings will be showed..	None
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.	None
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.	None
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...
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		None
Sign AuthnRequest	The samlp:AuthnRequest messages sent by this SP will be signed	None
Sign LogoutRequest	The samlp:logoutRequest messages sent by this SP will be signed	None
Sign LogoutResponse	The samlp:logoutResponse messages sent by this SP will be signed	None
Sign Metadata	The Metadata published by this SP will be signed	None

Option	Description	Default
Reject Unsigned Messages	Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received	None
Reject Unsigned Assertions	Reject unsigned saml:Assertion received	None
Reject Unencrypted Assertions	Reject unencrypted saml:Assertion received	None
Retrieve Parameters From Server	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-Redirect binding. Active this when you noticed signature validation failures, the plugin will try to extract the original query parameters.	None
Service Provider X.509 certificate	Public x509 certificate of the SP	None
Service Provider Private Key	Private key of the SP	None
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..	None

Log-in - Shibboleth

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database.	Disabled
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".	Disabled
Valid affiliations	A list of affiliations which will allow users to log in to this wiki 👆 *Separate multiple affiliations with commas*	None
Create with default group		Disabled

Option	Description	Default
Default group	The name of the default group	Shibboleth

Log-in - Webserver

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database.	Disabled