

# General Preferences

## Overview



Use this tab to configure your user registration and site security features.

## To Access

From the Login Config page, click the **General Preferences** tab.



Related Topics

- External Authentication

| Option                                   | Description   | Default  |
|--|---|----------|
| Authentication method                    | Tiki supports several authentication methods. The default method is to use the internal user database.<br> 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 on next login  | 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 - followed by a @ followed 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.<br> 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 |

| Option   | Description   | Default      |
|--|---|--------------|
| 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   | 👉 <i>Alphanumeric code required to complete the registration</i>  | None         |
| 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<br>👉 <i>Key required to be on included the URL to access the registration page (if not empty).</i>  | None         |
| Generate password  | Display a button on the registration form to automatically generate a very secure password for the user.<br>👉 <i>The generated password may not include any restrictions (such as minimum/maximum length).</i>  | 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.<br>☰ 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.<br>👉 <i>Choose a smaller number for less noise and easier reading.</i>   | 100          |
| Use reCAPTCHA  | Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA<br>👉 <i>You will need to register at <a href="http://www.google.com/recaptcha">http://www.google.com/recaptcha</a></i>   | 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.<br>☰ Clean   Black Glass   Red   White   | Clean        |

| Option  | Description   | Default  |
|---|---|----------|
| Version   | reCAPTCHA version.<br>☰ 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<br>👉 <i>One question per line with a colon separating the question and answer</i>   | None     |
| 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".<br>👉 <i>Default: tiki-information.php?msg=Account validated successfully.</i>  | 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.<br>👉 <i>Go to Admin Groups to select which tracker and fields to display.</i>  | 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     |

| Option   | Description  | Default  |
|--|--|----------|
| 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     |
| 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 system 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                          |  <i>Go to Admin Groups to select which tracker and fields to display.</i>   | 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.<br> <i>Use "-1" for never</i> | -1 days  |

| Option  | Description  | Default                        |
|---|--|--------------------------------|
| 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.<br>👉 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.<br>👉 Use "-1" for never  | 50 unsuccessful login attempts |
| 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.<br>👉 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.<br>⚠️ Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site  | Disabled                       |

| Option   | Description  | Default                    |
|--|--|----------------------------|
| Use HTTPS login  | <p>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.</p> <p>⚠️ <i>Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible</i></p> <p>☰ Disabled   Allow secure (HTTPS) login   Encourage secure (HTTPS) login   Consider we are always in HTTPS, but do not check   Require secure (HTTPS) login</p> | Allow secure (HTTPS) login |
| HTTP Basic Authentication                                  | <p>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</p> <p>☰ Disable   SSL Only (Recommended)   Always</p>   | Disable                    |
| 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  | <p>The port used to access this server; if not specified, port %0 will be used</p> <p>👉 <i>If not specified, port %0 will be used</i></p>  | 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  | <p>After logging in, users will automatically be logged in again when they leave and return to the site.</p> <p>☰ Disabled   User's choice   Always</p>  | User's choice              |
| Duration   | <p>The length of time before the user will need to log in again.</p> <p>☰ 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</p>   | 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  | <p>Name of the cookie to remember the user's login</p> <p>👉 <i>Changing the cookie name forces an instant logout for all user sessions. Including yours.</i></p>   | Tikiwiki                   |
| Domain   | The domain that the cookie is available to.  | None                       |

| Option                       | Description  | Default   |
|------------------------------|--|---|
| 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.<br>👉 <i>N.B. Needs to start with a / character to work properly in Safari</i>  | /   |
| Cookie Consent               | Ask permission of the user before setting any cookies, and comply with the response.<br>👉 <i>Complies with EU Privacy and Electronic Communications Regulations.</i> 🚫   | 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.<br>👉 <i>Wiki-parsed</i> 🚫  | privacy notice.">This website would like to ... |
| Cookie consent question      | Specific question next to the checkbox for agreement. Leave empty to not display a checkbox.<br>👉 <i>Wiki-parsed</i> 🚫   | 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.<br>👉 <i>Makes the checkbox opt in to accept "non-essential" cookies</i> 🚫 | 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<br>☰ 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  |

| Option   | Description   | Default                             |
|--|---|-------------------------------------|
| 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.<br><b>⚠️ Coverage will not be complete</b>   | 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                       |
| Force lowercase  | Automatically convert all alphabetic characters in the username to lowercase letters. For example <b>JohnDoe</b> becomes <b>johndoe</b> .   | Disabled                            |
| Username pattern   | This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /<br><code>'\-_a-zA-Z0-9@\.ת-ך*\$'/</code> or, for Chinese, use: /<br><code>'\-_a-zA-Z0-9@\.\\x00-\\xff*\$'/</code> | <code>/^\-_a-zA-Z0-9@\.*\$'/</code> |
| 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.<br><b>* Since passwords are stored securely, it's not possible to tell the user what the password is. It's only possible to change it.</b>                       | 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                                |



| Option   | Description   | Default      |
|--|---|--------------|
| 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     |
| 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.<br>👉 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     |

# CustomFields

A rudimentary capability exists to add additional text fields to the User Preferences page. This might be used for fields like:

- Home\_Phone
- AIM (or other IM handles)
- Address
- Professional\_Certs

In order to add a new field, you must insert a record into the tiki\_user\_preferences table manually (via phpMyadmin or...). Use a command similar to the following:

```
insert into tiki_user_preferences values('CustomFields','Home_Phone',NULL);
```

The values of the 3 fields are:

1. must be 'CustomFields'
2. descriptive label - this is what shows on screen as the field label
3. default value - NULL means no default, a string here will put that value in the field for the user to edit.

## Limits

1. At this time, there is no web page to create the actual field definitions, you must use the SQL statement shown above.
2. No spaces are allowed in the label, an underscore can be used instead.
3. There is no support for anything other than plain text fields
4. Possible security issue - if a user registers with the name 'CustomFields', they could

possibly change the default values, or cause other problems. Possible workaround - create your own user with that name and don't use it for anything.

5. The created fields are informational only, they don't hook into anything useful inside Tiki.

## Remember Me

If “User’s Choice” is selected the Login module will include a “Remember me” checkbox.

Without a rememberme cookie, the session finishes when the PHP session end. A session can finish because the idle time has been reached or the user closes their browser (or tab in the browser, depending on the browser).

With a rememberme cookie, you can extend the time the system remembers a user (if the user allows cookies and does not limit the cookie to the session time). This time is set in admin->login. When a user checks remember me checkbox, the browser creates a cookie with a name beginning with ‘tiki-user-’ followed by the rememberme name you gave in admin->login.

The rememberme feature allows you also to be able to close the browser and to be still logged in when you reopen the browser (if the timeout is not reached) The cookie is deleted when you log-out.

If the user changes their IP or browser, the Remember Me feature will fail.