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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication method</strong></td>
<td>Tiki supports several authentication methods. The default method is to use the internal user database. Tiki</td>
<td>Tiki</td>
</tr>
<tr>
<td></td>
<td>○ Tiki</td>
<td>Tiki and OpenID</td>
</tr>
<tr>
<td><strong>Intertiki</strong></td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Users can register</strong></td>
<td>Allow site visitors to register, using the registration form. The log-in module will include a &quot;Register&quot; link. If this is not activated, new users will have to be added manually by the admin on the Admin-Users page.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Validate new user registrations by email</strong></td>
<td>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.</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Validate user's email server</strong></td>
<td>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.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>○ No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Require validation by Admin</strong></td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Passcode</td>
<td>Alphanumeric code required to complete the registration</td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Registration page key</td>
<td>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).</td>
<td>None</td>
</tr>
<tr>
<td>Generate password</td>
<td>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).</td>
<td>None</td>
</tr>
<tr>
<td>Registration referrer check</td>
<td>Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Anonymous editors must enter anti-bot code (CAPTCHA)</td>
<td>Use CAPTCHA to ensure that anonymous input is from a person.</td>
<td>Enabled</td>
</tr>
<tr>
<td>CAPTCHA image word length</td>
<td>Number of characters the CAPTCHA will display.</td>
<td>6 characters</td>
</tr>
<tr>
<td>CAPTCHA image width</td>
<td>Width of the CAPTCHA image in pixels.</td>
<td>180 pixels</td>
</tr>
<tr>
<td>CAPTCHA image noise</td>
<td>Level of noise of the CAPTCHA image. Choose a smaller number for less noise and easier reading.</td>
<td>100</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| **Use reCAPTCHA**                          | Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA  
You will need to register at [http://www.google.com/recaptcha](http://www.google.com/recaptcha)                                                                                                                | Disabled         |
| **Site key**                                | **Description** reCAPTCHA public key obtained after registering.                                                                                                                                                                                                                                                                                | None             |
| **Secret key**                              | **Description** reCAPTCHA private key obtained after registering.                                                                                                                                                                                                                                                                             | None             |
| **reCAPTCHA theme**                        | **Description** Choose a theme for the reCAPTCHA widget.  
- Clean  
- Black Glass  
- Red  
- White                                                                                                                                                                                                                                                                         | Clean            |
| **Version**                                 | **Description** reCAPTCHA version.  
- 1.0  
- 2.0  
- 3.0                                                                                                                                                                                                                                                                                                                                   | 2.0              |
| **CAPTCHA questions**                      | **Description** Requires anonymous visitors to enter the answer to a question.                                                                                                                                                                                                                                                                | Disabled         |
| **CAPTCHA questions and answers**          | **Description** 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             |
| **Users must choose a group at registration** | **Description** Users cannot register without choosing one of the groups indicated above.                                                                                                                                                                                                                                                   | Disabled         |
| **URL the user is redirected to after account validation** | **Description** 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** | **Description** 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         |
<p>| <strong>Present different input fields in the User Wizard than are in the Registration form</strong> | <strong>Description</strong> Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form                                                                                                                                                                                                     | Disabled         |
| <strong>Tracker fields presented in the User Wizard as User Details</strong> | <strong>Description</strong> User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)                                                                                                                                                                                                         | None             |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use pretty trackers for registration form</strong></td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use a wiki page name or Smarty template file with a .tpl extension.</td>
<td>None</td>
</tr>
<tr>
<td>Hide Mandatory</td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name field ID</td>
<td>User the tracker's field ID whose value is used as the output page name.</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Select one or more trackers to sync user preferences from.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the &quot;real name&quot; pref from</td>
<td>Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using &quot;+&quot;, for example &quot;2+3,4&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation preferences with the main location field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Force users to upload an avatar.</td>
<td>Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require users to fill in tracker information</td>
<td>Require users to fill in a tracker form if not done already by prompting them with a modal dialog.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker ID of tracker required to be filled in</td>
<td>A tracker for articles must contain an &quot;Articles&quot; field.</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for required filling in</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.</td>
<td>None</td>
</tr>
<tr>
<td>Fields that are asked for in the modal for force-filling</td>
<td>Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested.</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Go to Admin Groups to select which tracker and fields to display.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user email after</td>
<td>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 &quot;-1&quot; for never</td>
<td>-1 days</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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 &quot;-1&quot; for never</td>
<td>20 unsuccessful login attempts</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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 &quot;,-1&quot; for never</td>
<td>50 unsuccessful login attempts</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>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</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>On permission denied, display login module</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent a session hijack through network sniffing. <strong>Warning:</strong> activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use HTTPS login</td>
<td>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server. <strong>Warning:</strong> do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible.</td>
<td>Allow secure (HTTPS) login</td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</td>
<td>Disable</td>
</tr>
<tr>
<td>Users can choose to stay in SSL mode after an HTTPS login</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can switch between secured or standard mode at login</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>HTTP port</td>
<td>The port used to access this server; if not specified, port 80 will be used. <em>If not specified, port 80 will be used</em></td>
<td>None</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>the HTTPS port for this server.</td>
<td>443</td>
</tr>
<tr>
<td>HTTPS for user-specific links</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>After logging in, users will automatically be logged in again when they leave and return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>The length of time before the user will need to log in again.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Refresh the remember-me cookie expiration</td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. <em>Changing the cookie name forces an instant logout for all user sessions. Including yours.</em></td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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. <em>N.B. Needs to start with a / character to work properly in Safari</em></td>
<td>/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask permission of the user before setting any cookies, and comply with the response. <em>Complies with EU Privacy and Electronic Communications Regulations.</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user's consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365 days</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog. <em>Wiki-parsed</em></td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. <em>Wiki-parsed</em>  ▶️</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.  ▶️</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.  ▶️</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Cookie consent mode           | Appearance of consent dialog  
*Dialog style requires feature_jquery_ui*  
[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                     |
| 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                     |
<p>| User emails must be unique    | The email address of each user must be unique.                                                                                                                                                              | Disabled                     |
| 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 <em>JohnDoe</em> becomes <em>johndoe</em>.                                                                                   | Disabled                     |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username pattern</td>
<td>This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: <code>/\-_a-zA-Z0-9@.א-ת/$</code> or, for Chinese, use: <code>/\-_a-zA-Z0-9@.\x00-\xff/$</code></td>
<td><code>/^[\-_a-zA-Z0-9@.]*$/</code></td>
</tr>
<tr>
<td>Auto-generate 6-digit username on registration</td>
<td>This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Forgot password               | Users can request a password reset. They will receive a link by email.  

[*Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.*]  

<p>| Allow users to use 2FA        | Allow users to enable Two-factor Authentication.                                                                                                                                                           | Disabled                                                                                      |
| 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 uppercase | Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;. 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 &quot; / $ % ? &amp; * ( ) _ + . 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 &quot;111&quot; or &quot;aab&quot;.                                                                                                         | Disabled                                                                                      |
| Prevent common passwords      | For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -&gt; Log in -&gt; Password Blacklist. | Disabled                                                                                      |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>The password must be different from the user's log-in name</td>
<td>The password must be different from the user's log-in name.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5 characters</td>
</tr>
<tr>
<td>Password expires after</td>
<td>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 &quot;-1&quot; for never</td>
<td>-1 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| Authentication method                            | Tiki supports several authentication methods. The default method is to use the internal user database.  

<table>
<thead>
<tr>
<th>Tiki</th>
<th>Tiki and OpenID</th>
<th>Tiki and PAM</th>
<th>Tiki and LDAP</th>
<th>CAS (Central Authentication Service)</th>
<th>Shibboleth</th>
<th>Web Server</th>
<th>phpBB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tiki</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users can register</td>
<td>Allow site visitors to register, using the registration form. The log-in module will include a &quot;Register&quot; link. If this is not activated, new users will have to be added manually by the admin on the Admin-Users page.</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>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.</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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.  

<table>
<thead>
<tr>
<th>No</th>
<th>Yes</th>
<th>Yes, with &quot;deep MX&quot; search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Validator emails</td>
<td>(separated by comma) if different than the sender email</td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>Users must enter an alphanumeric code to register. The site administrator</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>must inform users of this code. This is to restrict registration to invited</td>
<td></td>
</tr>
<tr>
<td></td>
<td>users.</td>
<td></td>
</tr>
<tr>
<td>Passcode</td>
<td><strong>Alphanumeric code required to complete the registration</strong></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>Displays the required passcode on the registration form. This is helpful</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>for legitimate users who want to register while making it difficult for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>automated robots because the passcode is unique for each site and because</td>
<td></td>
</tr>
<tr>
<td></td>
<td>it is displayed in JavaScript.</td>
<td></td>
</tr>
<tr>
<td>Registration page key</td>
<td>To register, users need to go to, for example: tiki-register.php?key=your</td>
<td>None</td>
</tr>
</tbody>
</table>
|                                      | registrationkeyvalue<br>
|                                      | *Key required to be on included the URL to access the registration page      |         |
|                                      | (if not empty).                                                            |         |
| Generate password                    | Display a button on the registration form to automatically generate a very  | Disabled|
|                                      | secure password for the user. <br>
<p>|                                      | <em>The generated password may not include any restrictions (such as          |         |
|                                      | minimum/maximum length.</em>                                                   |         |
| Registration referrer check          | Use the HTTP referrer to check registration POST is sent from same host.   | Enabled |
|                                      | (May not work on some setups.)                                              |         |
| Anonymous editors must enter         | Use CAPTCHA to ensure that anonymous input is from a person.               | Enabled |
| anti-bot code (CAPTCHA)              |                                                                            |         |
| CAPTCHA image word length            | Number of characters the CAPTCHA will display.                             | 6       |
| CAPTCHA image width                  | Width of the CAPTCHA image in pixels.                                      | 180     |
| CAPTCHA image noise                  | Level of noise of the CAPTCHA image. <em>Choose a smaller number for less    | 100     |
|                                      | noise and easier reading.</em>                                                  |         |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use reCAPTCHA</td>
<td>Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>You will need to register at</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.google.com/recaptcha">http://www.google.com/recaptcha</a></td>
<td></td>
</tr>
<tr>
<td>Site key</td>
<td>reCAPTCHA public key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>Secret key</td>
<td>reCAPTCHA private key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>reCAPTCHA theme</td>
<td>Choose a theme for the reCAPTCHA widget.</td>
<td>Clean</td>
</tr>
<tr>
<td></td>
<td>Clean</td>
<td>Black Glass</td>
</tr>
<tr>
<td>Version</td>
<td>reCAPTCHA version.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>1.0</td>
<td>2.0</td>
</tr>
<tr>
<td>CAPTCHA questions</td>
<td>Requires anonymous visitors to enter the answer to a question.</td>
<td>Disabled</td>
</tr>
<tr>
<td>CAPTCHA questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: &quot;Question?: Answer&quot; with one per line</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>One question per line with a colon separating the question and answer</td>
<td></td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>URL the user is redirected to after account validation</td>
<td>The default page a Registered user sees after account validation is &quot;tiki-information.php?msg=Account validated successfully&quot;. Default: tiki-information.php?msg=Account validated successfully.</td>
<td>None</td>
</tr>
<tr>
<td>Use a tracker to collect more user information</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Present different input fields in the User Wizard than are in the Registration form</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker fields presented in the User Wizard as User Details</td>
<td>User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use a wiki page name or Smarty template file with a .tpl extension.</td>
<td>None</td>
</tr>
<tr>
<td>Hide Mandatory</td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name field ID</td>
<td>User the tracker's field ID whose value is used as the output page name.</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Select one or more trackers to sync user preferences from.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the &quot;real name&quot; pref from</td>
<td>Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using &quot;+&quot;, for example &quot;2+3,4&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation preferences with the main location field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Force users to upload an avatar.</td>
<td>Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require users to fill in tracker information</td>
<td>Require users to fill in a tracker form if not done already by prompting them with a modal dialog.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker ID of tracker required to be filled in</td>
<td>A tracker for articles must contain an &quot;Articles&quot; field</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for required filling in</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.</td>
<td>None</td>
</tr>
<tr>
<td>Fields that are asked for in the modal for force-filling</td>
<td>Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Go to Admin Groups to select which tracker and fields to display.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user email after</td>
<td>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 &quot;-1&quot; for never.</td>
<td>-1 days</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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 &quot;-1&quot; for never.</td>
<td>20 unsuccessful login attempts</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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 &quot;-1&quot; for never.</td>
<td>50 unsuccessful login attempts</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>On permission denied, display login module</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent a session hijack through network sniffing. <strong>Warning:</strong> activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use HTTPS login</td>
<td>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server. <strong>Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible</strong></td>
<td>Allow secure (HTTPS) login</td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</td>
<td>Disable</td>
</tr>
<tr>
<td>Users can choose to stay in SSL mode after an HTTPS login</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can switch between secured or standard mode at login</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>HTTP port</td>
<td>The port used to access this server; if not specified, port 80 will be used. <strong>If not specified, port 80 will be used</strong></td>
<td>None</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>the HTTPS port for this server.</td>
<td>443</td>
</tr>
<tr>
<td>HTTPS for user-specific links</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>After logging in, users will automatically be logged in again when they leave and return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>The length of time before the user will need to log in again.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Refresh the remember-me cookie expiration</td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. <strong>Changing the cookie name forces an instant logout for all user sessions. Including yours.</strong></td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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. <strong>N.B. Needs to start with a / character to work properly in Safari</strong></td>
<td>/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask permission of the user before setting any cookies, and comply with the response. <strong>Complies with EU Privacy and Electronic Communications Regulations.</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user's consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365 days</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog. <strong>Wiki-parsed</strong></td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki-parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td>Cookie consent mode</td>
<td>Appearance of consent dialog Dialog style requires feature_jquery_ui</td>
<td>None</td>
</tr>
<tr>
<td>Cookie consent dialog ID</td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Cookie consent disabled</td>
<td>Do not give the option to refuse cookies but still inform the user about cookie usage.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Banning system</td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use email as username</td>
<td>Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Obscure email when using email as username</td>
<td>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</td>
<td>Disabled</td>
</tr>
<tr>
<td>User emails must be unique</td>
<td>The email address of each user must be unique.</td>
<td>Disabled</td>
</tr>
<tr>
<td>User can login via username or email</td>
<td>This will allow users to login using their email (as well as their username).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid username.</td>
<td>1 characters</td>
</tr>
<tr>
<td>Maximum length</td>
<td>The greatest number of characters for a valid username.</td>
<td>50 characters</td>
</tr>
<tr>
<td>Force lowercase</td>
<td>Automatically convert all alphabetic characters in the username to lowercase letters. For example JohnDoe becomes JohnDoe.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Username pattern</td>
<td>This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /- _a-zA-Z0-9@\n-\n*$/ or, for Chinese, use: /- _a-zA-Z0-9@\x00-\xff*$/</td>
<td>/^[ -_a-zA-Z0-9@]*$/</td>
</tr>
<tr>
<td>Auto-generate 6-digit username on registration</td>
<td>This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Forgot password</td>
<td>Users can request a password reset. They will receive a link by email.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;. Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; * ( ) _ + . Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as &quot;111&quot; or &quot;aab&quot;.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent common passwords</td>
<td>For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -&gt; Log in -&gt; Password Blacklist.</td>
<td>Disabled</td>
</tr>
<tr>
<td>The password must be different from the user's log-in name</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5 characters</td>
</tr>
<tr>
<td>Password expires after</td>
<td>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 &quot;-1&quot; for never</td>
<td>-1 days</td>
</tr>
</tbody>
</table>
| Authentication method        | Tiki supports several authentication methods. The default method is to use the internal user database.  

| Tiki | Tiki and OpenID | Tiki and PAM | Tiki and LDAP | CAS (Central Authentication Service) | Shibboleth | Web Server | phpBB |
| Authentication method        | Tiki supports several authentication methods. The default method is to use the internal user database.  

| Tiki | Tiki and OpenID | Tiki and PAM | Tiki and LDAP | CAS (Central Authentication Service) | Shibboleth | Web Server | phpBB |
| Intertiki                     | Allows several Tiki sites (slaves) to get authentication from a master Tiki site.                                                                                                                             | 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.  

<p>| No | Yes | Yes, with &quot;deep MX&quot; search |
| 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 |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><strong>Alphanumeric code required to complete the registration</strong></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| 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       |
| 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.                              | 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      |
<p>| Site key                           | reCAPTCHA public key obtained after registering.                             | None          |
| Secret key                         | reCAPTCHA private key obtained after registering.                            | None          |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>reCAPTCHA theme</td>
<td>Choose a theme for the reCAPTCHA widget.</td>
<td>Clean</td>
</tr>
<tr>
<td></td>
<td>Clean</td>
<td>Black Glass</td>
</tr>
<tr>
<td>Version</td>
<td>reCAPTCHA version.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>1.0</td>
<td>2.0</td>
</tr>
<tr>
<td>CAPTCHA questions</td>
<td>Requires anonymous visitors to enter the answer to a question.</td>
<td>Disabled</td>
</tr>
<tr>
<td>CAPTCHA questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: &quot;Question?: Answer&quot; with one per line.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>One question per line with a colon separating the question and answer</td>
<td></td>
</tr>
<tr>
<td>Users must choose a group at</td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>registration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL the user is redirected to after</td>
<td>The default page a Registered user sees after account validation is &quot;tiki-information.php?msg=Account validated successfully&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Use a tracker to collect more user</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>information</td>
<td>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td></td>
</tr>
<tr>
<td>Present different input fields in</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>the User Wizard than are in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration form</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracker fields presented in the</td>
<td>User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)</td>
<td>None</td>
</tr>
<tr>
<td>User Wizard as User Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker</td>
<td>Use a wiki page name or Smarty template file with a .tpl extension.</td>
<td>None</td>
</tr>
<tr>
<td>template</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Hide Mandatory</td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name field ID</td>
<td>User the tracker's field ID whose value is used as the output page name.</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the comma-separated IDs of trackers to sync user preferences from.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the &quot;real name&quot; pref from</td>
<td>Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using &quot;+&quot;, for example &quot;2+3,4&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation preferences with the main location field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Force users to upload an avatar.</td>
<td>Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require users to fill in tracker information</td>
<td>Require users to fill in a tracker form if not done already by prompting them with a modal dialog.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Tracker ID of tracker required to be filled in</td>
<td>A tracker for articles must contain an &quot;Articles&quot; field</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for required filling in</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.</td>
<td>None</td>
</tr>
<tr>
<td>Fields that are asked for in the modal for force-filling</td>
<td>Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested</td>
<td>None</td>
</tr>
<tr>
<td><strong>Use tracker to collect more group information</strong></td>
<td>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user email after</td>
<td>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. <em>Use &quot;-1&quot; for never</em></td>
<td>-1 days</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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. <em>Use &quot;-1&quot; for never</em></td>
<td>20 unsuccessful login attempts</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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. <em>Use &quot;-1&quot; for never</em></td>
<td>50 unsuccessful login attempts</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Automatically create a group for each user in order to, for example, assign permissions on the individual-user level. <em>The group name will be the same as the user's username</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>On permission denied, display login module</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent a session hijack through network sniffing. <strong>Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>Use HTTPS login</td>
<td>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server. <strong>Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible</strong></td>
<td>Allow secure (HTTPS) login</td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</td>
<td>Disable</td>
</tr>
<tr>
<td>Users can choose to stay in SSL mode after an HTTPS login</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can switch between secured or standard mode at login</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>HTTP port</td>
<td>The port used to access this server; if not specified, port 80 will be used. <strong>If not specified, port 80 will be used</strong></td>
<td>None</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>the HTTPS port for this server.</td>
<td>443</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>HTTPS for user-specific links</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>After logging in, users will automatically be logged in again when they leave and return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>The length of time before the user will need to log in again.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Refresh the remember-me cookie expiration</td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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</td>
<td>/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask permission of the user before setting any cookies, and comply with the response. Complies with EU Privacy and Electronic Communications Regulations.  ▶️</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user's consent if the user agrees.  ▶️</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).  ▶️</td>
<td>365 days</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog. Wiki-parsed  ▶️</td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki-parsed  ▶️</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.  ▶️</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Cookie consent mode                      | Appearance of consent dialog
|                                          | *Dialog style requires feature_jquery_ui*                                   | None            |
|                                          | ⚠️ Plain | Banner | Dialog ❓               |
| 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        |
| 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        |
| 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 JohnDoe becomes john doe. | Disabled        |
| Username pattern                         | This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /
<p>|                                          | ⌂_a-zA-Z0-9@.,-*$/ or, for Chinese, use: /_a-zA-Z0-9@\x00-\xff*$/ | /^[ _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        |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgot password</td>
<td>Users can request a password reset. They will receive a link by email. <em>Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.</em></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;. Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; ( ) _ + . Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as &quot;111&quot; or &quot;aab&quot;.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent common passwords</td>
<td>For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -&gt; Log in -&gt; Password Blacklist.</td>
<td>Disabled</td>
</tr>
<tr>
<td>The password must be different from the user's log-in name</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5 characters</td>
</tr>
<tr>
<td>Password expires after</td>
<td>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. <em>Use &quot;-1&quot; for never</em></td>
<td>-1 days</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Tiki supports several authentication methods. The default method is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td></td>
<td>Tiki</td>
<td>Tiki and OpenID</td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Users can register</td>
<td>Allow site visitors to register, using the registration form. The log-in module will include a &quot;Register&quot; link. If this is not activated, new users will have to be added manually by the admin on the Admin-Users page.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>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.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate user's email server</td>
<td>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.</td>
<td>No</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><em>Alphanumeric code required to complete the registration</em></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 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 |
| 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.                                                                                                                                                            | 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 this security service provided by Google instead of the 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                                                                                                                                                    | 2.0     |
<p>| CAPTCHA questions                                | Requires anonymous visitors to enter the answer to a question.                                                                                                                                               | Disabled|</p>
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
<th><strong>Default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPTCHA questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: &quot;Question?: Answer&quot; with one per line. <em>One question per line with a colon separating the question and answer</em></td>
<td>None</td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>URL the user is redirected to after account validation</td>
<td>The default page a Registered user sees after account validation is &quot;tiki-information.php?msg=Account validated successfully&quot;. <em>Default: tiki-information.php?msg=Account validated successfully.</em></td>
<td>None</td>
</tr>
<tr>
<td>Use a tracker to collect more user information</td>
<td>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. <em>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Present different input fields in the User Wizard than are in the Registration form</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker fields presented in the User Wizard as User Details</td>
<td>User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)</td>
<td>None</td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use a wiki page name or Smarty template file with a .tpl extension.</td>
<td>None</td>
</tr>
<tr>
<td>Hide Mandatory</td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name field ID</td>
<td>User the tracker's field ID whose value is used as the output page name.</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the comma-separated IDs of trackers to sync user preferences from.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the &quot;real name&quot; pref from</td>
<td>Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using &quot;+&quot;, for example &quot;2+3,4&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation preferences with the main location field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Force users to upload an avatar.</td>
<td>Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require users to fill in tracker information.</td>
<td>Require users to fill in a tracker form if not done already by prompting them with a modal dialog</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker ID of tracker required to be filled in</td>
<td>A tracker for articles must contain an &quot;Articles&quot; field.</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for required filling in</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Fields that are asked for in the modal for force-filling</td>
<td>Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user email after</td>
<td>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 &quot;-1&quot; for never</td>
<td>-1 days</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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 &quot;-1&quot; for never</td>
<td>20 unsuccessful login attempts</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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 &quot;-1&quot; for never</td>
<td>50 unsuccessful login attempts</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>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</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. This will cause the user to be logged out</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 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

| 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

| HTTP Basic Authentication            | Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.  

≡ Disable | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login

| Users can choose to stay in SSL mode after an HTTPS login |  

| Users can switch between secured or standard mode at login |  

| HTTP port                              | The port used to access this server; if not specified, port 80 will be used  

If not specified, port 80 will be used

| HTTPS port                             | the HTTPS port for this server.  

| 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.  

| Remember me                            | After logging in, users will automatically be logged in again when they leave and return to the site.  

≡ Disable | User’s choice | Always

| Duration                               | The length of time before the user will need to log in again.  

≡ 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year

<p>| Enable | 2 hours  |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the remember-me cookie expiration</td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login &lt;br&gt;&lt;i&gt;Changing the cookie name forces an instant logout for all user sessions. Including yours.&lt;/i&gt;</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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. &lt;br&gt;&lt;i&gt;N.B. Needs to start with a / character to work properly in Safari&lt;/i&gt;</td>
<td>/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask permission of the user before setting any cookies, and comply with the response. &lt;br&gt;&lt;i&gt;Complies with EU Privacy and Electronic Communications Regulations.&lt;/i&gt;</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user's consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365 days</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog.</td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. &lt;br&gt;Leave empty to not display a checkbox. &lt;br&gt;&lt;i&gt;Wiki-parsed&lt;/i&gt;</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies. &lt;br&gt;&lt;i&gt;Wiki-parsed&lt;/i&gt;</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td>Cookie consent mode</td>
<td>Appearance of consent dialog &lt;br&gt;&lt;i&gt;Dialog style requires feature_jquery_ui&lt;/i&gt;</td>
<td>None</td>
</tr>
<tr>
<td>Cookie consent dialog ID</td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Cookie consent disabled</td>
<td>Do not give the option to refuse cookies but still inform the user about cookie usage.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Banning system</strong></td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Use email as username</strong></td>
<td>Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Obscure email when using email as username</strong></td>
<td>As much as possible, attempt to not display the email address, showing the real name or the truncated email address instead. <strong>(\textbf{\textsc{Coverage will not be complete}})</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>User emails must be unique</strong></td>
<td>The email address of each user must be unique.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>User can login via username or email.</strong></td>
<td>Allow users to log in using their email address (as well as their username).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid username.</td>
<td>1 characters</td>
</tr>
<tr>
<td>Maximum length</td>
<td>The greatest number of characters for a valid username.</td>
<td>50 characters</td>
</tr>
<tr>
<td><strong>Force lowercase</strong></td>
<td>Automatically convert all alphabetic characters in the username to lowercase letters. For example <strong>JohnDoe</strong> becomes <strong>johndoe</strong>.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| 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@\.\n-\x00-\xff]*$/ or for Chinese use: /
\[-\_a-zA-Z0-9@\.\x00-\xff]*$/ | /^\[-\_a-zA-Z0-9@\.]*$/ |
<p>| 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 |
| <strong>Forgot password</strong>             | Users can request a password reset. They will receive a link by email.     | Enabled |
|                                 | <strong>(\textbf{\textit{Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.}})</strong>                                                                 |         |
| <strong>Users can change their password</strong> | Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin. | Enabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;. Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; ( ) _ + . Use this option to require users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as &quot;111&quot; or &quot;aab&quot;.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent common passwords</td>
<td>For improved security, prevent passwords in your password blacklist from being used.</td>
<td>Disabled</td>
</tr>
<tr>
<td>The password must be different from the user's log-in name</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5 characters</td>
</tr>
<tr>
<td>Password expires after</td>
<td>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 forced to select a new password when logging in. Use &quot;-1&quot; for never</td>
<td>-1 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Tiki supports several authentication methods. The default method is to use the internal user database. ☻ Tiki</td>
<td>Tiki</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tiki and OpenID</td>
</tr>
<tr>
<td></td>
<td>Intertiki Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Users can register</td>
<td>This will allow users to register, using the webform. The Login module will include a Register link. If disabled, the admin will have to create new users manually on the Admin Users page.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>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.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate user’s email server</td>
<td>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.</td>
<td>No</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><em>Alphanumeric code required to complete the registration</em></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Registration page key          | for example, to register, users need to go to: tiki-register.php?key=yourregistrationkeyvalue  
*Key required to be on included the URL to access the registration page (if not empty).* | None      |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate password</td>
<td>Tiki will include a button on the registration form that will automatically generate a very secure password for the user. <em>The generated password may not include any restrictions (such as minimum/maximum length).</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration referrer check</td>
<td>Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Anonymous editors must enter anti-bot code (CAPTCHA)</strong></td>
<td>Use CAPTCHA to ensure that anonymous input is from a person.</td>
<td>Enabled</td>
</tr>
<tr>
<td>CAPTCHA image word length</td>
<td>Number of characters the CAPTCHA will display.</td>
<td>6 characters</td>
</tr>
<tr>
<td>CAPTCHA image width</td>
<td>Width of the CAPTCHA image in pixels.</td>
<td>180 pixels</td>
</tr>
<tr>
<td>CAPTCHA image noise</td>
<td>Level of noise of the CAPTCHA image. <em>Choose a smaller number for less noise and easier reading.</em></td>
<td>100</td>
</tr>
<tr>
<td><strong>Use ReCaptcha</strong></td>
<td>Use ReCaptcha, a specialized captcha service, instead of default CAPTCHA</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>You will need to register at <a href="http://www.google.com/recaptcha">http://www.google.com/recaptcha</a></td>
<td></td>
</tr>
<tr>
<td>Site key</td>
<td>ReCaptcha public key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>Secret key</td>
<td>ReCaptcha private key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>ReCaptcha theme</td>
<td>Choose a theme for the ReCaptcha widget.</td>
<td>Clean</td>
</tr>
<tr>
<td></td>
<td>[Clean</td>
<td>Black Glass</td>
</tr>
<tr>
<td>Version</td>
<td>ReCaptcha version.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>[1.0</td>
<td>2.0](#)</td>
</tr>
<tr>
<td>CAPTCHA questions</td>
<td>Requires anonymous visitors to enter the answer to a question.</td>
<td>Disabled</td>
</tr>
<tr>
<td>CAPTCHA questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: “Question?: Answer” with one per line <em>One question per line with a colon separating the question and answer</em></td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>Users must choose a group at registration</strong></td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>URL the user is redirected to after account validation</strong></td>
<td>The default page a Registered user sees after account validation is <code>tiki-information.php?msg=Account validated successfully</code>. Default: <code>tiki-information.php?msg=Account validated successfully</code>.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Use a tracker to collect more user information</strong></td>
<td>Display a tracker (form) for the user to complete as part of the registration process. This tracker will be used to store additional information about each user. Go to the “Admin Groups” page to select which tracker and fields to display.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Present different input fields in the User Wizard than are in the Registration form</strong></td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Tracker fields presented in the User Wizard as User Details</strong></td>
<td>User’s information tracker fields presented in the User Wizard as User Details (separate fieldIds with colons)</td>
<td>None</td>
</tr>
<tr>
<td><strong>Use pretty trackers for registration form</strong></td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Registration pretty tracker template</strong></td>
<td>Use wiki page name or template file with .tpl extension</td>
<td>None</td>
</tr>
<tr>
<td><strong>Hide Mandatory</strong></td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Output the registration results</strong></td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Output registration pretty tracker template</strong></td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td><strong>Page name field ID</strong></td>
<td>User tracker’s field ID whose value is used as output page name</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the IDs separated by commas of trackers to sync user prefs from</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the “real name”</td>
<td>Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the IDs separated by commas of all fields that contain group names to sync user groups to</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation prefs to main location field</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>tracker item language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a user tracker item when registering</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>force email equals this field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Force users to upload an avatar.</td>
<td>Forces a user to upload an avatar if they haven’t already by prompting them with a modal</td>
<td>Disabled</td>
</tr>
<tr>
<td>Force users to fill tracker information.</td>
<td>Forces a user to fill in a tracker form if they haven’t already by prompting them with a module</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker ID of tracker for force-filling</td>
<td>The tracker that is for articles must contain an “Articles” field</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not</td>
<td>None</td>
</tr>
<tr>
<td>force-filling</td>
<td>completed it.</td>
<td></td>
</tr>
<tr>
<td>Fields that are asked for in the modal for</td>
<td>Comma-separated permnames of fields that are asked for in the modal for force-filling. If empty, all fields are</td>
<td>None</td>
</tr>
<tr>
<td>force-filling</td>
<td>asked for</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Go to the “Admin Groups” page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user email after</td>
<td>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. <em>Use “-1” for never</em></td>
<td>-1 days</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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. <em>Use “-1” for never</em></td>
<td>20 unsuccessful login attempts</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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. <em>Use “-1” for never</em></td>
<td>50 unsuccessful login attempts</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Tiki will automatically create a group for the user. <em>The group name will be the same as the user’s username</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Disable browser’s autocomplete feature for username and password fields</td>
<td>Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent a session hijack through network sniffing. <em>Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
| **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** | Allow secure (HTTPS) login |
| **HTTP Basic Authentication**               | Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.  
  **IDS: Disabled | SSL Only (Recommended) | Always**                                                                                                                                  | Disable                  |
| Users can choose to stay in SSL mode after an HTTPS login |                                                                                                                                                                                                           | Enabled                  |
| Users can switch between secured or standard mode at login |                                                                                                                                                                                                           | Disabled                 |
| **HTTP port**                               | The port used to access this server; if not specified, port 80 will be used  
  **If not specified, port 80 will be used**                                                                                                        | None                     |
| **HTTPS port**                              | the HTTPS port for this server.                                                                                                                                                                             | 443                      |
| Use HTTPS when building user-specific links | When building notification emails, RSS feeds 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**                             | Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.  
  **IDS: Disabled | User’s choice | Always**                                                                                                                                   | Disabled                 |
| **Duration**                                | You can define the length of time that Tiki will “remember” the user.  
  **IDS: 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year**                                                                 | 2 hours                  |
| 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.                                                                                        | Disabled                 |
| **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                 |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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. <em>N.B. Needs to start with a / character to work properly in Safari</em></td>
<td>/</td>
</tr>
<tr>
<td><strong>Cookie Consent</strong></td>
<td>Ask permission of the user before setting any cookies, and comply with the response. <em>Complies with EU Privacy and Electronic Communications Regulations.</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user’s consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365 days</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog. <em>Wiki-parsed</em></td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. <em>Wiki-parsed</em></td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td>Cookie consent mode</td>
<td>Appearance of consent dialog <em>Dialog style requires feature_jquery_ui</em></td>
<td>None</td>
</tr>
<tr>
<td>Cookie consent dialog ID</td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Cookie consent disabled</td>
<td>Do not give the option to refuse cookies but still inform the user about cookie usage.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Banning system</td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use email as username</td>
<td>Instead of creating new usernames, use the user’s email address for authentication. On the registration form, there will be no Username field.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Obscure email when using email as username</td>
<td>This will attempt as much as possible to hide the email address, showing the real name or the truncated email address instead. <strong>⚠️ Coverage will not be complete</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>User emails must be unique</td>
<td>User e-mails must be unique</td>
<td>Disabled</td>
</tr>
<tr>
<td>User can login via username or email.</td>
<td>This will allow users to login using their email (as well as their username).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid username.</td>
<td>1 characters</td>
</tr>
<tr>
<td>Maximum length</td>
<td>The greatest number of characters for a valid username.</td>
<td>50 characters</td>
</tr>
<tr>
<td>Force lowercase</td>
<td>Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example <strong>JohnDoe</strong> becomes <strong>johndoe</strong>.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Username pattern</td>
<td>This regex pattern force and forbid the use fo certain characters for username. For example to add Hebrew use: <code>/^-a-zA-Z0-9@\&amp;\#46;א-ת/</code> or for Chinese use: <code>/-a-zA-Z0-9@\&amp;\#46;\x00-\xff/$/</code></td>
<td><code>/^\[ '\-_a-zA-Z0-9@\.]*$/</code></td>
</tr>
<tr>
<td>Auto-generate 6-digit username on registration</td>
<td>This will auto-generate a 6-digit username for users who sign up (they will normally login with emails only).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Forgot password</td>
<td>Users can request a password reset. They will receive a link by email. <strong>✨ Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like “a” and one uppercase character like “A”. Use this option to force users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like ”/ $ % ? * ( ) _ + . Use this option to force users to select stronger passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as “111” or “aab”.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent common passwords</td>
<td>For improved security, prevent passwords in your password blacklist from being used.</td>
<td>Disabled</td>
</tr>
<tr>
<td>The password must be different from the user’s log-in name</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5 characters</td>
</tr>
<tr>
<td>Password expires after</td>
<td>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 forced to select a new password when logging in. Use “-1” for never</td>
<td>-1 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Tiki supports several authentication methods. The default method is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Users can register</td>
<td>Permit user registration</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>Upon registration, the new user will receive an email containing a new-account validation link.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Validate user's email server</td>
<td>Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><em>Alphanumeric code required to complete the registration</em></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Registration page key                       | For example, to register, users need to go to: tiki-register.php?key=yourregistrationkeyvalue  
*Key required to be on included the URL to access the registration page (if not empty).*                                                                 | None     |
| Generate password                           | Include "Generate password" option in registration form  
*The generated password may not include any restrictions (such as minimum/maximum length).*                                                                                                           | Disabled |
<p>| Registration referrer check                 | Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)                                                                                                   | Enabled  |
| Anonymous editors must enter anti-bot code (CAPTCHA) | Use CAPTCHA to ensure that anonymous input is from a person                                                                                                                                               | Enabled  |
| Word length of the CAPTCHA image            | Word length of the CAPTCHA image. Default:6                                                                                                                                                               | 6        |
| Width of the CAPTCHA image in pixels        | Width of the CAPTCHA image in pixels. Default:180                                                                                                                                                        | 180      |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of noise of the CAPTCHA image</td>
<td>Level of noise of the CAPTCHA image. Choose a smaller number for less noise and easier reading. Default: 100</td>
<td></td>
</tr>
<tr>
<td>Use ReCaptcha</td>
<td>Use ReCaptcha, a specialized captcha service, instead of default CAPTCHA</td>
<td>Disabled</td>
</tr>
<tr>
<td>Site key</td>
<td>ReCaptcha public key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>Secret key</td>
<td>ReCaptcha private key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>ReCaptcha theme</td>
<td>Choose a theme for the ReCaptcha widget.</td>
<td>Clean</td>
</tr>
<tr>
<td>Version</td>
<td>ReCaptcha version.</td>
<td>2.0</td>
</tr>
<tr>
<td>CAPTCHA Questions</td>
<td>Requires anonymous visitors to enter the answer to a question.</td>
<td>Disabled</td>
</tr>
<tr>
<td>CAPTCHA Questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: &quot;Question?: Answer&quot; with one per line.</td>
<td></td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>URL the user is redirected to after account validation</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Use a tracker to collect more user information</td>
<td>Display a tracker (form) for the user to complete as part of the registration process. This tracker will be used to store additional information about each user. Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Present different input fields in the User Wizard than are in the Registration form</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Tracker fields presented in the User Wizard as User Details</td>
<td>User's information tracker fields presented in the User Wizard as User Details (separate fieldIds with colons)</td>
<td>None</td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use wiki page name or template file with .tpl extension</td>
<td>None</td>
</tr>
<tr>
<td>Hide Mandatory</td>
<td>Hide mandatory fields indication with an asterisk (shown by default).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name field ID</td>
<td>User tracker's field ID whose value is used as output page name</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the IDs separated by commas of trackers to sync user prefs from</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync the &quot;real name&quot; pref from</td>
<td>Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync user groups</td>
<td>Enter the IDs separated by commas of all fields that contain group names to sync user groups to</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation prefs to main location field</td>
<td>Disabled</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Force users to upload an avatar.</strong></td>
<td>Forces a user to upload an avatar if they haven't already by prompting them with a modal</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Force users to fill tracker information.</strong></td>
<td>Forces a user to fill in a tracker form if they haven't already by prompting them with a module</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracker ID of tracker for force-filling</td>
<td>The tracker that is for articles must contain an &quot;Articles&quot; field</td>
<td>None</td>
</tr>
<tr>
<td>Mandatory tracker field to check for force-filling</td>
<td>The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.</td>
<td>None</td>
</tr>
<tr>
<td>Fields that are asked for in the modal for force-filling</td>
<td>Comma-separated permnames of fields that are asked for in the modal for force-filling. If empty, all fields are asked for</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td><em>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>Number of days to wait before re-validating the user's email address. <em>Use &quot;-1&quot; for never days</em></td>
<td>-1</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>After a certain number of consecutive unsuccessful login 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. <em>Use &quot;-1&quot; for never unsuccessful login attempts</em></td>
<td>20</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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. <em>Use &quot;-1&quot; for never unsuccessful login attempts</em></td>
<td>50</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Tiki will automatically create a group for the user. <em>The group name will be the same as the user's username</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent a session hijack through network sniffing. <strong>⚠️ Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>Use HTTPS login</td>
<td>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server. <strong>⚠️ Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible</strong></td>
<td>Allow secure (HTTPS) login</td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</td>
<td>Disable</td>
</tr>
<tr>
<td>Users can choose to stay in SSL mode after an HTTPS login</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can switch between secured or standard mode at login</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>HTTP port</td>
<td>The port used to access this server; if not specified, port 80 will be used. <strong>If not specified, port 80 will be used</strong></td>
<td>None</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>the HTTPS port for this server, default=443 <strong>If left empty, port 443 will be used</strong></td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Use HTTPS when building user-specific links</td>
<td>When building notification emails, RSS feeds or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>You can define the length of time that Tiki will “remember” the user.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Refresh the remember-me cookie expiration</td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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</td>
<td>/tiki16/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask permission of the user before setting any cookies, and comply with the response. Complies with EU Privacy and Electronic Communications Regulations.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie consent name</td>
<td>Name of the cookie to record the user's consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie consent expiration</td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365</td>
</tr>
<tr>
<td>Cookie consent text</td>
<td>Description for the dialog. Wiki-parsed</td>
<td>This website would like to ...</td>
</tr>
<tr>
<td>Cookie consent question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki-parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Cookie consent alert</td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie consent button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Cookie consent mode | Appearance of consent dialog  
*Dialog style requires feature_jquery_ui*  
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 |
| Use email as username | Instead of creating new usernames, use the user's email address for authentication. | Disabled |
| Obscure the email address when using the email address as username if possible (coverage will not be complete) | 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 |
<p>| User e-mails must be unique | User e-mails must be unique | Disabled |
| User can login via username or e-mail. | 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 |
| Maximum length | The greatest number of characters for a valid username. | 50 |
| Force lowercase | Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example <em>JohnDoe</em> becomes <em>johndoe</em>. | Disabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username pattern</td>
<td>This regex pattern force and forbid the use fo certain characters for username. For example to add Hebrew use: / ^[^-_a-zA-Z0-9@.]<em>$/ or for Chinese use: / ^[^-_a-zA-Z0-9@.\x00-\xff]</em>$/</td>
<td>/^[^-_a-zA-Z0-9@.]*$/</td>
</tr>
<tr>
<td>Auto-generate 6-digit username on registration</td>
<td>This will auto-generate a 6-digit username for users who sign up (they will normally login with emails only).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Forgot password</td>
<td>Users can request a password reset. They will receive a link by email.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Allow users to change their own login password</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot;/ $ % &amp; ( ) _ + ...</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as &quot;111&quot; or &quot;aab&quot;.</td>
<td>Disabled</td>
</tr>
<tr>
<td>The password must be different from the user's log-in name</td>
<td>The password must be different from the user's log-in name.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5</td>
</tr>
<tr>
<td>Password expires after</td>
<td>password expiry period (in days)</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>Use &quot;-1&quot; for never days</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Authentication method</strong></td>
<td>Tiki supports several authentication methods. The default method is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Users can register</td>
<td>Permit user registration</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>Upon registration, the new user will receive an email containing a new-account validation link.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate user's email server</td>
<td>Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><strong>Alphanumeric code required to complete the registration</strong></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration page key</td>
<td>for example, to register, users need to go to: tiki-register.php?key=yourregistrationkeyvalue Key required to be on included the URL to access the registration page (if not empty).</td>
<td>None</td>
</tr>
<tr>
<td>Generate password</td>
<td>Include &quot;Generate password&quot; option in registration form The generated password may not include any restrictions (such as minimum/maximum length.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration referrer check</td>
<td>Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Anonymous editors must enter anti-bot code (CAPTCHA)</td>
<td>Use CAPTCHA to ensure that anonymous input is from a person</td>
<td>Enabled</td>
</tr>
<tr>
<td>Word length of the CAPTCHA image</td>
<td>Word length of the CAPTCHA image. Default:6</td>
<td>6</td>
</tr>
<tr>
<td>Width of the CAPTCHA image in pixels</td>
<td>Width of the CAPTCHA image in pixels. Default:180</td>
<td>180</td>
</tr>
<tr>
<td>Level of noise of the CAPTCHA image</td>
<td>Level of noise of the CAPTCHA image. Choose a smaller number for less noise and easier reading. Default:100 Choose a smaller number for less noise and easier reading.</td>
<td>100</td>
</tr>
<tr>
<td>Use ReCaptcha</td>
<td>Use ReCaptcha, a specialized captcha service, instead of default CAPTCHA You will need to register at <a href="http://www.google.com/recaptcha">http://www.google.com/recaptcha</a></td>
<td>Disabled</td>
</tr>
<tr>
<td>Public Key</td>
<td>ReCaptcha public key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>Private Key</td>
<td>ReCaptcha private key obtained after registering.</td>
<td>None</td>
</tr>
<tr>
<td>ReCaptcha theme</td>
<td>Choose a theme for the ReCaptcha widget.</td>
<td>Clean</td>
</tr>
<tr>
<td>Version</td>
<td>ReCaptcha version.</td>
<td>2.0</td>
</tr>
<tr>
<td>CAPTCHA Questions</td>
<td>Requires anonymous visitors to enter the answer to a question.</td>
<td>Disabled</td>
</tr>
<tr>
<td>CAPTCHA Questions and answers</td>
<td>Add some simple questions that only humans should be able to answer, in the format: &quot;Question?: Answer&quot; with one per line One question per line with a colon separating the question and answer</td>
<td>None</td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups indicated above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>URL the user is redirected to after account validation</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| **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 be used to store additional information about each user.  
*Go to the "Admin Groups" page to select which tracker and fields to display* | Disabled |
<p>| <strong>Present different input fields in the User Wizard than are in the Registration form</strong> | Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form | Disabled |
| <strong>Tracker fields presented in the User Wizard as User Details</strong> | User's information tracker fields presented in the User Wizard as User Details (separate fieldIds with colons) | None     |
| <strong>Use pretty trackers for registration form</strong>               | Use pretty trackers for registration form                                     | Disabled |
| <strong>Registration pretty tracker template</strong>                    | Use wiki page name or template file with .tpl extension                      | None     |
| <strong>Hide Mandatory</strong>                                         | Hide mandatory fields indication with an asterisk (shown by default).        | Disabled |
| <strong>Output the registration results</strong>                        | Use a wiki page as template to output the registration results to             | Disabled |
| <strong>Output registration pretty tracker template</strong>             | Wiki page only                                                              | None     |
| <strong>Page name field ID</strong>                                     | User tracker's field ID whose value is used as output page name              | None     |
| <strong>User tracker IDs to sync prefs from</strong>                    | Enter the IDs separated by commas of trackers to sync user prefs from        | None     |
| <strong>Tracker field IDs to sync the &quot;real name&quot; pref from</strong>    | Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4 | None     |
| <strong>Synchronize long/lat/zoom to location field</strong>            | Synchronize user geolocation prefs to main location field                    | Disabled |
| <strong>Change user system language when changing user tracker item language</strong> |                                                                      | Disabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Go to the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>Number of days to wait before re-validating the user's email address. Use &quot;-1&quot; for never days.</td>
<td>-1</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>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 &quot;-1&quot; for never unsuccessful login attempts.</td>
<td>20</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>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 &quot;-1&quot; for never unsuccessful login attempts</td>
<td>50</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Tiki will automatically create a group for the user. The group name will be the same as the user's username.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use challenge/response authentication</td>
<td>Confirm that the Admin account has a valid email address or you will not be able to log in.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prevent multiple log-ins by the same user</td>
<td>Users (other than admin) cannot log in simultaneously with multiple browsers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Grab session if already logged in</td>
<td>If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| 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**  
|  | Disable | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login |
| HTTP Basic Authentication                   | Check credentials from HTTP Basic Authentication, which is useful to allow webservice to use credentials.                                                                                                    | Disable                   |
| Users can choose to stay in SSL mode after an HTTPS login |                                                                                                                                                                                                               | Enabled                   |
| Users can switch between secured or standard mode at login |                                                                                                                                                                                                               | Disabled                  |
| HTTP port                                  | The port used to access this server; if not specified, port 80 will be used  
*If not specified, port 80 will be used*                                                                                                                                                                         | None                      |
| HTTPS port                                 | the HTTPS port for this server, default=443  
*If left empty, port 443 will be used*                                                                                                                                                                             | None                      |
| Use HTTPS when building user-specific links | When building notification emails, RSS feeds 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                                | Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.  
<p>|  | Disable | User's choice | Always |
|</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Duration</strong></td>
<td>You can define the length of time that Tiki will “remember” the user.</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 minutes</td>
</tr>
<tr>
<td><strong>Refresh the remember-me cookie expiration</strong></td>
<td>Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Cookie name</strong></td>
<td>Name of the cookie to remember the user's login Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>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</td>
<td>/tiki15/</td>
</tr>
<tr>
<td><strong>Cookie Consent</strong></td>
<td>Ask permission of the user before setting any cookies, and comply with the response. Complies with EU Privacy and Electronic Communications Regulations.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Cookie consent name</strong></td>
<td>Name of the cookie to record the user's consent if the user agrees.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td><strong>Cookie consent expiration</strong></td>
<td>Expiration date of the cookie to record consent (in days).</td>
<td>365</td>
</tr>
<tr>
<td><strong>Cookie consent text</strong></td>
<td>Description for the dialog. Wiki-parsed</td>
<td>This website would like to ...</td>
</tr>
<tr>
<td><strong>Cookie consent question</strong></td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki-parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td><strong>Cookie consent alert</strong></td>
<td>Alert displayed when user tries to access or use a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td><strong>Cookie consent button</strong></td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td><strong>Cookie consent mode</strong></td>
<td>Appearance of consent dialog Dialog style requires feature_jquery_ui</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Plain</td>
<td>Banner</td>
</tr>
<tr>
<td><strong>Cookie consent dialog ID</strong></td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Cookie consent disabled</td>
<td>Do not give the option to refuse cookies but still inform the user about cookie usage. ▶️</td>
<td>Disabled</td>
</tr>
<tr>
<td>Banning system</td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use email as username</td>
<td>Instead of creating new usernames, use the user's email address for authentication.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Obscure the email address when using the email address as username if possible (coverage will not be complete)</td>
<td>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</td>
<td>Disabled</td>
</tr>
<tr>
<td>User e-mails must be unique</td>
<td>User e-mails must be unique</td>
<td>Disabled</td>
</tr>
<tr>
<td>User can login via username or e-mail.</td>
<td>This will allow users to login using their email (as well as their username).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid username.</td>
<td>1</td>
</tr>
<tr>
<td>Maximum length</td>
<td>The greatest number of characters for a valid username.</td>
<td>50</td>
</tr>
<tr>
<td>Force lowercase</td>
<td>Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example <strong>JohnDoe</strong> becomes <strong>johndoe</strong>.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Username pattern</td>
<td>This regex pattern force and forbid the use fo certain characters for username. For example to add Hebrew use: /[-_a-zA-Z0-9@&amp;#46;\n-\x*$/ or for Chinese use: /[-_a-zA-Z0-9@&amp;#46;\x00-\xff*$/</td>
<td>/^['_-a-zA-Z0-9@&amp;#46;\n-\x*$/</td>
</tr>
<tr>
<td>Auto-generate 6-digit username on registration</td>
<td>This will auto-generate a 6-digit username for users who sign up (they will normally login with emails only).</td>
<td>Disabled</td>
</tr>
<tr>
<td>Store password as plain text</td>
<td>Users can request a password reset. They will receive a link by email.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Forgot password</td>
<td>Users can request a password reset. They will receive a link by email.</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>✴️ Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Encryption method</td>
<td><strong>crypt-md5</strong></td>
<td><strong>crypt-des</strong></td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Allow users to change their own login password</td>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of alphabetical characters and numerals in passwords.</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one lowercase alphabetical character like &quot;a&quot; and one uppercase character like &quot;A&quot;.</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; * ( ) _ + ...&quot;</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must not contain a consecutive repetition of the same character such as &quot;111&quot; or &quot;aab&quot;.</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>The password must be different from the user's log-in name</td>
<td>The password must be different from the user's log-in name.</td>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td><strong>5</strong></td>
</tr>
<tr>
<td>Password expires after</td>
<td><strong>Use &quot;-1&quot; for never days</strong></td>
<td><strong>-1</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Tiki supports several authentication methods. The default value is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Users can register</td>
<td>permit User registration</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>Upon registration, the new user will receive an email containing a link to confirm validity.</td>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td>Validate user's email server</td>
<td>Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.</td>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can login.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>Users must enter a code to register. You must inform users of this code. Use to restrict registration to invited users only.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><em>Alphanumeric code required to complete the registration</em></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Registration Page Key                          | `e.g. To register users need to go to: tiki-register.php?key=yourregistrationkeyvalue
 `*Key required to be on included the URL to access the registration page (if not empty).*` | None     |
| Generate Password                               | Include "Generate Password" option on registration form
 *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  |
| Users must choose a group at registration       | Users cannot register without choosing one of the groups defined above.        | Disabled |
| URL a 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     |
<p>| Use tracker to collect more user information   | Display a tracker (form) for the user to complete, as part of the registration process. Use this tracker to store additional information about each user. <em>Use the &quot;Admin Groups&quot; page to select which tracker and fields to display</em> | Disabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask different fields in the User Wizard than the ones in Registration</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Enabled</td>
</tr>
<tr>
<td>Tracker Fields Asked in the User Wizard as User Details</td>
<td>Users Information Tracker Fields Asked in the User Wizard as User Details (fieldIds separated with colon)</td>
<td>None</td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use wiki page name or template file with .tpl extension</td>
<td>None</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name fieldId</td>
<td>User trackers field id whose value is used as output page name</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the IDs separated by commas of trackers to sync user prefs from</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync Real Name pref from</td>
<td>Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4</td>
<td>None</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation prefs to main location field</td>
<td>Disabled</td>
</tr>
<tr>
<td>Synchronize categories of user tracker item to user groups</td>
<td>Will add the user tracker item to the category of the same name as the user groups and vice versa</td>
<td>Disabled</td>
</tr>
<tr>
<td>Put user in group only if categorized within</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td><em>Use the &quot;Admin Groups&quot; page to select which tracker and fields to display</em></td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Re-validate user by email after                     | number of days to wait before re-validating the User's email  
*Use "-1" for never days*                                                                                                                                                                             | -1      |
| Re-validate user by email after                     | After a certain number of consecutive unsuccessfull login attempts, the user will receive a mail with instruction to validate his account. However the user can still log-in with his old password.  
*Use "-1" for never unsuccessful login attempts*                                                                                                                                               | 20      |
| Suspend account after                               | After a certain number of consecutive unsuccessfull login attempts, the account is suspended. An admin must revalidate the account before the user can use it again.  
*Use "-1" for never unsuccessful login attempts*                                                                                                                                              | -1      |
| Create a new group for each user                    | Tiki will automatically create a group for the user.  
*The group will be named identical to the user's username*                                                                                                                                              | Disabled|
| Disable browser's autocomplete feature for username and password fields | Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites. | Disabled|
| Use challenge/response authentication                | *Confirm that the Admin account has a valid email address or you will not be permitted to login  
⚠️ Deprecated: This feature is unmaintained and may not be reliable*                                                                                                                                 | Disabled|
<p>| Prevent multiple logins from same user             | User can not login simultaneously from multiple browsers. Admin account is still allowed.                                                                                                                                 | Disabled|</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect all sessions with HTTPS</td>
<td>Always redirect to HTTPS to prevent session hijack through network sniffing.</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>✅ Only activate if you have already configured SSL, otherwise, your will lock yourself out of Tiki</td>
<td></td>
</tr>
<tr>
<td>Use HTTPS login</td>
<td>Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.</td>
<td>Allow secure (https) login</td>
</tr>
<tr>
<td></td>
<td>🟠 Do not require HTTPS until you have setup and tested the connection, otherwise, you will make your whole site unaccessible</td>
<td></td>
</tr>
<tr>
<td>HTTP Basic Authentication</td>
<td>Check credentials from HTTP Basic Authentication, useful to allow webservices to use credentials.</td>
<td>Disable</td>
</tr>
<tr>
<td></td>
<td>✒ Disable</td>
<td>SSL Only (Recommended)</td>
</tr>
<tr>
<td>Users can choose to stay in SSL mode after an HTTPS login</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>Users can switch between secured or standard mode at login</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>HTTP port</td>
<td>the port used to access this server, if left empty will use port 80</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>✅ If left empty, port 80 will be used</td>
<td></td>
</tr>
<tr>
<td>HTTPS port</td>
<td>the HTTPS port for this server, default=443</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>✅ If left empty, port 443 will be used</td>
<td></td>
</tr>
<tr>
<td>Use HTTPS when building user-specific links</td>
<td>When building notification emails, RSS feeds or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>✒ Disabled</td>
<td>User's choice</td>
</tr>
<tr>
<td>Duration</td>
<td>You can define the length of time that Tiki will “remember” the user.</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td>✒ 5 minutes</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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. <em>N.B. Needs to start with a / character to work properly in Safari</em></td>
<td>/12/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask users permission before setting any cookies, and obey their decision. Complies with EU Privacy and Electronic Communications Regulations.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie Consent Name</td>
<td>Name of the cookie to record consent if they agree.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie Consent Expiry</td>
<td>Expiry date for the cookie to record consent (in days).</td>
<td>365</td>
</tr>
<tr>
<td>Cookie Consent Text</td>
<td>Description for the dialog. Wiki parsed</td>
<td>This site would like to pla...</td>
</tr>
<tr>
<td>Cookie Consent Question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie Consent Alert</td>
<td>Alert displayed when user tries to access a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie Consent Button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td>Cookie Consent Mode</td>
<td>Appearance of consent dialog Dialog style requires feature_jquery_ui</td>
<td>None</td>
</tr>
<tr>
<td>Cookie Consent Dialog Id</td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Banning system</td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use email as username</td>
<td>Instead of creating new usernames, use the user's email address for authentication.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Obscure email when using email as username if possible (coverage will not be complete) | This will attempt as much as possible to hide the email, showing the realname or the truncated email instead.  
**⚠️ Coverage will not be complete**  
This will attempt as much as possible to hide the email, showing the realname or the truncated email instead. | Disabled |
| Minimum length                                                      | The least possible number of characters for a valid username.                                                                                                                                               | 1        |
| Maximum length                                                      | The greatest number of characters for a valid username.                                                                                                                                                     | 50       |
| Force lowercase                                                      | Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example *JohnDoe* becomes *johndoe*.                                                            | Disabled |
| Username pattern                                                     | This regex pattern force and forbid the use fo certain characters for username. For example to add Hebrew use: / *'-_a-zA-Z0-9@.א-ת*/  
For Chinese use: / *'-_a-zA-Z0-9@.\x00-\xff*/ | /^[ '-_a-zA-Z0-9@.]*$/ |
| Store password as plain text                                        |                                                                                                                                                                                                           | Disabled |
| Forgot password                                                      | Users can request to reset password. They will receive a link by email.  
**⚠️ Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.** | Enabled  |
<p>| Encryption method                                                   | *crypt-md5 | crypt-des | tikihash (old)                                                                                           | crypt-md5 |
| Users can change their password                                     | Allow users to change their own login password                                                                                                                                                    | Enabled  |
| Require characters and numerals                                     | For improved security, require users to include a mix of characters and numerals in passwords.                                                                                                         | Disabled |
| Require alphabetical characters in lower and upper case             | Password must contain at least one alphabetical character in lower case like a and one in upper case like A.                                                                                           | Disabled |
| Require special characters                                          | Password must contain at least one special character in lower case like &quot; / $ % ? &amp; * ( ) _ + ...                                                                                                        | Disabled |
| Require no consecutive repetition of the same character              | Password must contain no consecutive repetition of the same character as 111 or aab.                                                                                                                     | Disabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password must be different from the user login</td>
<td>Password must be different from the user login.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5</td>
</tr>
<tr>
<td>Password expires after password expiry period (in days)</td>
<td>Use &quot;-1&quot; for never days</td>
<td>-1</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Tiki supports several authentication methods. The default value is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td></td>
<td>Tiki</td>
<td>Tiki and OpenID</td>
</tr>
<tr>
<td>Intertiki</td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Users can register</td>
<td>permit User registration</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>Upon registration, the new user will receive an email containing a link to confirm validity.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate user’s email server</td>
<td>Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can login.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails (separated by comma) if different than the sender email</td>
<td>^None^</td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>Users must enter a code to register. You must inform users of this code. Use to restrict registration to invited users only.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td>Alphanumeric code required to complete the registration</td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Registration Page Key       | e.g. To register users need to go to: tiki-register.php?key=yourregistrationkeyvalue
Key required to be on included the URL to access the registration page (if not empty). | None    |
| Generate Password           | Include "Generate Password" option on registration form
The generated password may not include any restrictions (such as minimum/maximum length.) | Disabled |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration referrer check</td>
<td>Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups defined above.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| URL a 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 tracker to collect more user information | Display a tracker (form) for the user to complete, as part of the registration process. Use this tracker to store additional information about each user.  
*Use the “Admin Groups” page to select which tracker and fields to display* | Disabled|
<p>| Ask different fields in the User Wizard than the ones in Registration | Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form | Enabled |
| Tracker Fields Asked in the User Wizard as User Details | Users Information Tracker Fields Asked in the User Wizard as User Details (fieldIds separated with colon) | None    |
| Use pretty trackers for registration form   | Use pretty trackers for registration form                                      | Disabled|
| Registration pretty tracker template        | Use wiki page name or template file with .tpl extension                       | None    |
| 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 fieldId                          | User trackers field id whose value is used as output page name                 | None    |
| User tracker IDs to sync prefs from         | Enter the IDs separated by commas of trackers to sync user prefs from          | None    |
| Tracker field IDs to sync Real Name pref from | Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4 | None    |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation prefs to main location field</td>
<td>Disabled</td>
</tr>
<tr>
<td>Synchronize categories of user tracker item to user groups</td>
<td>Will add the user tracker item to the category of the same name as the user groups and vice versa</td>
<td>Disabled</td>
</tr>
<tr>
<td>Put user in group only if categorized within</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Use the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>number of days to wait before re-validating the User's email</td>
<td>-1</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>After a certain number of consecutive unsuccessfull login attempts, the user will receive a mail with instruction to validate his account. However the user can still log-in with his old password. Use &quot;-1&quot; for never unsuccessful login attempts</td>
<td>20</td>
</tr>
<tr>
<td>Suspend account after</td>
<td>After a certain number of consecutive unsuccessfull login attempts, the account is suspended. An admin must revalidate the account before the user can use it again. Use &quot;-1&quot; for never unsuccessful login attempts</td>
<td>-1</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Tiki will automatically create a group for the user. The group will be named identical to the user's username</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Use challenge/response authentication                                 | Confirm that the Admin account has a valid email address or you will not be permitted to login  
⚠️ Deprecated: This feature is unmaintained and may not be reliable                                                                                                                                      | Disabled                  |
| Prevent multiple logins from same user                               | User can not login simultaneously from multiple browsers. Admin account is still allowed.                                                                                                                    | Disabled                  |
| Protect all sessions with HTTPS                                      | Always redirect to HTTPS to prevent session hijack through network snifing.  
⚠️ Only activate if you have already configured SSL, otherwise, your will lock yourself out of Tiki                                                                                                  | 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 you have setup and tested the connection, otherwise, you will make your whole site unaccessible  
≡ 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, useful to allow webservices to use credentials.  
≡ Disable | SSL Only (Recommended) | Always                                                                                                                                  | Disable                  |
| Users can choose to stay in SSL mode after an HTTPS login            |                                                                                                                                                                                                        | Enabled                   |
| Users can switch between secured or standard mode at login           |                                                                                                                                                                                                        | Disabled                  |
| HTTP port                                                           | the port used to access this server, if left empty will use port 80  
If left empty, port 80 will be used                                                                                                                                             | None                      |
| HTTPS port                                                          | the HTTPS port for this server, default=443  
If left empty, port 443 will be used                                                                                                                                            | None                      |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use HTTPS when building user-specific links</td>
<td>When building notification emails, RSS feeds or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>You can define the length of time that Tiki will “remember” the user.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user’s login. Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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.</td>
<td><code>/12/</code></td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask users permission before setting any cookies, and obey their decision. Complies with EU Privacy and Electronic Communications Regulations.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie Consent Name</td>
<td>Name of the cookie to record consent if they agree.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie Consent Expiry</td>
<td>Expiry date for the cookie to record consent (in days).</td>
<td>365</td>
</tr>
<tr>
<td>Cookie Consent Text</td>
<td>Description for the dialog. Wiki parsed</td>
<td>This site would like to pla...</td>
</tr>
<tr>
<td>Cookie Consent Question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie Consent Alert</td>
<td>Alert displayed when user tries to access a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie Consent Button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Cookie Consent Mode</td>
<td>Appearance of consent dialog</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td><em>Dialog style requires feature_jquery_ui</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plain</td>
<td>Banner</td>
</tr>
<tr>
<td>Cookie Consent Dialog Id</td>
<td>DOM id for the dialog container div.</td>
<td>Cookie_consent_div</td>
</tr>
<tr>
<td>Banning system</td>
<td>Deny access to specific users based on username, IP, and date/time range.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Use email as username</td>
<td>Instead of creating new usernames, use the user's email address for authentication.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Obscure email when using email as username if possible (coverage will not be complete)</td>
<td>This will attempt as much as possible to hide the email, showing the realname or the truncated email instead.</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Coverage will not be complete</em></td>
<td></td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid username.</td>
<td>1</td>
</tr>
<tr>
<td>Maximum length</td>
<td>The greatest number of characters for a valid username.</td>
<td>50</td>
</tr>
<tr>
<td>Force lowercase</td>
<td>Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example <strong>JohnDoe</strong> becomes <strong>johndoe</strong>.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Username pattern</td>
<td>This regex pattern force and forbid the use of certain characters for username. For example to add Hebrew use: / ^[-_a-zA-Z0-9@.]<em>$/ or for Chinese use: / ^[-_a-zA-Z0-9@&amp;#46;\x00-\xff]</em>$/</td>
<td></td>
</tr>
<tr>
<td>Store password as plain text</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Forgot password</td>
<td>Users can request to reset password. They will receive a link by email.</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td><em>Since passwords are encrypted, it's not possible to tell the user what the password is. It's only possible to change it.</em></td>
<td></td>
</tr>
<tr>
<td>Encryption method</td>
<td>*crypt-md5</td>
<td>crypt-des</td>
</tr>
<tr>
<td>Users can change their password</td>
<td>Allow users to change their own login password</td>
<td>Enabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one alphabetical character in lower case like a and one in upper case like A.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; * ( ) _ + ...</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must contain no consecutive repetition of the same character as 111 or aab.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Password must be different from the user login</td>
<td>Password must be different from the user login.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5</td>
</tr>
</tbody>
</table>
| Password expires after                      | password expiry period (in days)  
*Use "-1" for never days* | -1      |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication method</strong></td>
<td>Tiki supports several authentication methods. The default value is to use the internal user database.</td>
<td>Tiki</td>
</tr>
<tr>
<td></td>
<td>☐ Tiki</td>
<td>☐ Tiki and OpenID</td>
</tr>
<tr>
<td><strong>Intertiki</strong></td>
<td>Allows several Tiki sites (slaves) to get authentication from a master Tiki site</td>
<td>Disabled</td>
</tr>
<tr>
<td>Users can register</td>
<td>permit User registration</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validate new user registrations by email</td>
<td>Upon registration, the new user will receive an email containing a link to confirm validity.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate user's email server</td>
<td>Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require validation by Admin</td>
<td>The administrator will receive an email for each new user registration, and must validate the user before the user can login.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Validator emails</td>
<td>None (separated by comma) if different than the sender email</td>
<td>None</td>
</tr>
<tr>
<td>Require passcode to register</td>
<td>Users must enter a code to register. You must inform users of this code. Use to restrict registration to invited users only.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passcode</td>
<td><em>Alphanumeric code required to complete the registration</em></td>
<td>None</td>
</tr>
<tr>
<td>Show passcode on registration form</td>
<td>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.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Registration Page Key             | e.g. To register users need to go to: tiki-register.php?key=yourregistrationkeyvalue  
**Key required to be on included the URL to access the registration page (if not empty).** | None     |
| Generate Password                  | Include "Generate Password" option on registration form  
*The generated password may not include any restrictions (such as minimum/maximum length).* | Disabled |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration referrer check</td>
<td>Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Users must choose a group at registration</td>
<td>Users cannot register without choosing one of the groups defined above.</td>
<td>Disabled</td>
</tr>
<tr>
<td>URL a user is redirected to after account validation</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more user information</td>
<td>Display a tracker (form) for the user to complete, as part of the registration process. Use this tracker to store additional information about each user. <em>Use the &quot;Admin Groups&quot; page to select which tracker and fields to display</em></td>
<td>Disabled</td>
</tr>
<tr>
<td>Ask different fields in the User Wizard than the ones in Registration</td>
<td>Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form</td>
<td>Enabled</td>
</tr>
<tr>
<td>Tracker Fields Asked in the User Wizard as User Details</td>
<td>Users Information Tracker Fields Asked in the User Wizard as User Details (fieldIds separated with colon)</td>
<td>None</td>
</tr>
<tr>
<td>Use pretty trackers for registration form</td>
<td>Use pretty trackers for registration form</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registration pretty tracker template</td>
<td>Use wiki page name or template file with .tpl extension</td>
<td>None</td>
</tr>
<tr>
<td>Output the registration results</td>
<td>Use a wiki page as template to output the registration results to</td>
<td>Disabled</td>
</tr>
<tr>
<td>Output registration pretty tracker template</td>
<td>Wiki page only</td>
<td>None</td>
</tr>
<tr>
<td>Page name fieldId</td>
<td>User trackers field id whose value is used as output page name</td>
<td>None</td>
</tr>
<tr>
<td>User tracker IDs to sync prefs from</td>
<td>Enter the IDs separated by commas of trackers to sync user prefs from</td>
<td>None</td>
</tr>
<tr>
<td>Tracker field IDs to sync Real Name pref from</td>
<td>Enter the IDs separated by commas in priority of being chosen, each item can concatenate multiple fields using +, e.g. 2+3,4</td>
<td>None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Synchronize long/lat/zoom to location field</td>
<td>Synchronize user geolocation prefs to main location field</td>
<td>Disabled</td>
</tr>
<tr>
<td>Synchronize categories of user tracker item to user groups</td>
<td>Will add the user tracker item to the category of the same name as the user groups and vice versa</td>
<td>Disabled</td>
</tr>
<tr>
<td>Put user in group only if categorized within</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Change user system language when changing user tracker item language</td>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>Assign a user tracker item when registering if email equals this field</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Use tracker to collect more group information</td>
<td>Use the &quot;Admin Groups&quot; page to select which tracker and fields to display</td>
<td>Disabled</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>number of days to wait before re-validating the User's email</td>
<td>-1</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>After a certain number of consecutive unsuccessful login attempts, the user will receive a mail with</td>
<td>20</td>
</tr>
<tr>
<td>Re-validate user by email after</td>
<td>instruction to validate his account. However the user can still log-in with his old password.</td>
<td></td>
</tr>
<tr>
<td>Suspend account after</td>
<td>After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin</td>
<td>-1</td>
</tr>
<tr>
<td>Create a new group for each user</td>
<td>Tiki will automatically create a group for the user. The group will be named identical to the user's</td>
<td>Disabled</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Disable browser's autocomplete feature for username and password fields</td>
<td>Use to deactivate the autocomplete in the login 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 login and password can not be remembered. You should enable this feature for highly secure sites.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Use challenge/response authentication                                    | Confirm that the Admin account has a valid email address or you will not be permitted to login

⚠️ Deprecated: This feature is unmaintained and may not be reliable

| Prevent multiple logins from same user                                 | User can not login simultaneously from multiple browsers. Admin account is still allowed.                                                                                                                     | Disabled                 |
| Protect all sessions with HTTPS                                       | Always redirect to HTTPS to prevent session hijack through network sniffing.

⚠️ Only activate if you have already configured SSL, otherwise, your will lock yourself out of Tiki

| 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 you have setup and tested the connection, otherwise, you will make your whole site unaccessible

-disabled | Allow secure (https) login | Encourage secure (https) login | Consider we are always in HTTPS, but do not check | Require secure (https) login |

| HTTP Basic Authentication                                              | Check credentials from HTTP Basic Authentication, useful to allow webservices to use credentials.                                                                                                           | Disable                  |
| Users can choose to stay in SSL mode after an HTTPS login              |                                                                                                                                                                                                             | Enabled                  |
| Users can switch between secured or standard mode at login             |                                                                                                                                                                                                             | Disabled                 |
| HTTP port                                                             | the port used to access this server, if left empty will use port 80

*If left empty, port 80 will be used*

| HTTPS port                                                            | the HTTPS port for this server, default=443

*If left empty, port 443 will be used*                                                                                  | None                      |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use HTTPS when building user-specific links</td>
<td>When building notification emails, RSS feeds or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remember me</td>
<td>Use this option to have Tiki remember users. They will automatically be logged in if they leave, then return to the site.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Duration</td>
<td>You can define the length of time that Tiki will “remember” the user.</td>
<td>2 hours</td>
</tr>
<tr>
<td>Cookie name</td>
<td>Name of the cookie to remember the user's login. Changing the cookie name forces an instant logout for all user sessions. Including yours.</td>
<td>Tikiwiki</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain that the cookie is available to.</td>
<td>None</td>
</tr>
<tr>
<td>Path</td>
<td>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</td>
<td>/12/</td>
</tr>
<tr>
<td>Cookie Consent</td>
<td>Ask users permission before setting any cookies, and obey their decision. Complies with EU Privacy and Electronic Communications Regulations.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cookie Consent Name</td>
<td>Name of the cookie to record consent if they agree.</td>
<td>Tiki_cookies_accepted</td>
</tr>
<tr>
<td>Cookie Consent Expiry</td>
<td>Expiry date for the cookie to record consent (in days).</td>
<td>365</td>
</tr>
<tr>
<td>Cookie Consent Text</td>
<td>Description for the dialog. Wiki parsed</td>
<td>This site would like to pla...</td>
</tr>
<tr>
<td>Cookie Consent Question</td>
<td>Specific question next to the checkbox for agreement. Leave empty to not display a checkbox. Wiki parsed</td>
<td>I accept cookies from this ...</td>
</tr>
<tr>
<td>Cookie Consent Alert</td>
<td>Alert displayed when user tries to access a feature requiring cookies.</td>
<td>Sorry, cookie consent required</td>
</tr>
<tr>
<td>Cookie Consent Button</td>
<td>Label on the agreement button.</td>
<td>Continue</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Cookie Consent Mode              | Appearance of consent dialog<br>
*Dialog style requires feature_jquery_ui*<br> Plain | Banner | Dialog | None |
| Cookie Consent Dialog Id         | DOM id for the dialog container div.                                            | Cookie_consent_div |
| Banning system                   | Deny access to specific users based on username, IP, and date/time range.      | Disabled |
| Use email as username            | Instead of creating new usernames, use the user's email address for authentication. | Disabled |
| Obscure email when using email as username if possible (coverage will not be complete) | This will attempt as much as possible to hide the email, showing the realname or the truncated email instead.  ▲ Coverage will not be complete | Disabled |
| Minimum length                   | The least possible number of characters for a valid username.                  | 1           |
| Maximum length                   | The greatest number of characters for a valid username.                        | 50          |
| Force lowercase                  | Tiki will automatically convert all alphabetic characters in the username to all lowercase letters. For example JohnDoe becomes johndoe. | Disabled |
| Username pattern                 | This regex pattern force and forbid the use fo certain characters for username. For example to add Hebrew use: / [-a-zA-Z0-9@&

<p>| Store password as plain text     |                                                                                | Disabled |
| Forgot password                  | Users can request to reset password. They will receive a link by email.        | Enabled |
| Encryption method                |  crypt-md5 | crypt-des | tikihash (old) | crypt-md5 | |
| Users can change their password  | Allow users to change their own login password                                | Enabled |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require characters and numerals</td>
<td>For improved security, require users to include a mix of characters and numerals in passwords.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require alphabetical characters in lower and upper case</td>
<td>Password must contain at least one alphabetical character in lower case like a and one in upper case like A.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require special characters</td>
<td>Password must contain at least one special character in lower case like &quot; / $ % ? &amp; * ( ) _ + ...</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require no consecutive repetition of the same character</td>
<td>Password must contain no consecutive repetition of the same character as 111 or aab.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Password must be different from the user login</td>
<td>Password must be different from the user login.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The least possible number of characters for a valid password.</td>
<td>5</td>
</tr>
<tr>
<td>Password expires after</td>
<td>Password expiry period (in days)</td>
<td>-1</td>
</tr>
</tbody>
</table>

**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:

```sql
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.
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.