General Preferences

Overview

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

To Access

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

Related Topics

- External Authentication

Option

Authentication method

Intertiki

Description

Tiki supports several authentication methods. The default method is to use the internal user database.

Tiki | Tiki and OpenID Connect | Tiki and PAM | Tiki and LDAP | CAS (Central Authentication Service) | Shibboleth | Web Server | phpBB

Allows several Tiki sites (slaves) to get authentication from a master Tiki site

Default

Tiki

Disabled

Option

User must change password set default on

Users can register

Description

Set default value for the 'user must change password at next login' checkbox in the registration form when adding new user by the admin. This is to avoid to have to check the said checkbox everytime on next user's creation if your policy is that the new user must change the password given by the admin at next login.

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.

Default

Disabled

Disabled

Option

Validate new user registrations by email

Description

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.

Default

Enabled

Option

Validate user's email server

Require validation by Admin

Description

Tiki will attempt to validate the userâ€™s email address by examining the syntax of the email address. It must be a string of letters, or digits or _ or . or - follows by a @ follows by a string of letters, or digits or _ or . or -. Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.

☰ No | Yes | Yes, with "deep MX" search

The administrator will receive an email for each new user registration, and must validate the user before the user can log in.

Default

No

Disabled

Option

Validator emails (separated by comma) if different than the sender email

Require passcode to register

Passcode

Description

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.

👆 *Alphanumeric code required to complete the registration*

Default

None

Disabled

None

Option

Show passcode on registration form

Registration page key

Description

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.

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).*

Default

Disabled

None

Option

Generate password

Registration referrer check

Display Disposable Emails

Description

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.*

Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)

Show if a user's email address is from a disposable / temporary email address provider

Default

Disabled

Enabled

Disabled

Option

Anonymous editors must enter anti-bot code (CAPTCHA)

CAPTCHA image word length

CAPTCHA image width

CAPTCHA image noise

Description

Use CAPTCHA to ensure that anonymous input is from a person.

Number of characters the CAPTCHA will display.

Width of the CAPTCHA image in pixels.

Level of noise of the CAPTCHA image.
👆 *Choose a smaller number for less noise and easier reading.*

Default

Enabled

6 characters

180 pixels

100

Option

Use reCAPTCHA

Site key

Secret key

reCAPTCHA theme

Version

Description

Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA

👆 *You will need to register at*

http://www.google.com/recaptcha

reCAPTCHA public key obtained after registering.

reCAPTCHA private key obtained after registering.

Choose a theme for the reCAPTCHA widget.

☰ Clean | Black Glass | Red | White

reCAPTCHA version.

☰ 1.0 | 2.0 | 3.0

Default

Disabled

None

None

Clean

2.0

Option

CAPTCHA questions

CAPTCHA questions and answers

Users must choose a group at registration

Description

Requires anonymous visitors to enter the answer to a question.

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*

Users cannot register without choosing one of the groups indicated above.

Default

Disabled

None

Disabled

Option

URL the user is redirected to after account validation

Use a tracker to collect more user information

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.*

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.*

Default

None

Disabled

Option

Add a user tracker item for new user set default on

Present different input fields in the User Wizard than are in the Registration form

Tracker fields presented in the User Wizard as User Details

Description

Set default value for the "add a user tracker item for this user" checkbox in the registration form when adding new user by the admin. This is to avoid to have to check the said checkbox everytime on next users creation if your policy is that you want to add a tracker item in the user tracker when creating a new user.

Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form

User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)

Default

Disabled

Disabled

None

Option

Use pretty trackers for registration form

Registration pretty tracker template

Hide Mandatory

Output the registration results

Output registration pretty tracker template

Description

Allows a site manager to design forms using registration fields and have the results of each field displayed in customizable way on a Wiki page or Smarty template.

Use a wiki page name or Smarty template file with a .tpl extension.

Hide mandatory fields indication with an asterisk (shown by default).

Use a wiki page as template to output the registration results to

Wiki page only

Default

Disabled

None

Disabled

Disabled

None

Option

Page name field ID

User tracker IDs to sync prefs from

Tracker field IDs to sync the "real name" pref from

Tracker field IDs to sync user groups

Description

User the tracker's field ID whose value is used as the output page name.

Select one or more trackers to sync user preferences from.

Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using "+", for example "2+3,4".

Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.

Default

None

None

None

None

Option

Synchronize long/lat/zoom to location field

Change user system language when changing user tracker item language

Assign a user tracker item when registering if email equals this field

Force users to upload an avatar.

Description

Synchronize user geolocation preferences with the main location field.

Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.

Default

Disabled

Disabled

None

Disabled

Option

Require users to fill in tracker information

Tracker ID of tracker required to be filled in

Mandatory tracker field to check for required filling in

Fields that are asked for in the modal for force-filling

Description

Require users to fill in a tracker form if not done already by prompting them with a modal dialog.

A tracker for articles must contain an "Articles" field

The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.

Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested

Default

Disabled

None

None

None

Option

Use tracker to collect more group information

Re-validate user email after

Description

👆 *Go to Admin Groups to select which tracker and fields to display.*

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 userâ€™s email is still valid.

👆 *Use "-1" for never*

Default

Disabled

-1 days

Option

Re-validate user by email after

Suspend/lockout account after

Description

After a certain number of consecutive unsuccessful log-in attempts, the user will receive an email with instruction to validate his or her account. However, the user can still log in with the old password.

👆 *Use "-1" for never*

After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin must revalidate the account before the user can use it again.

👆 *Use "-1" for never*

Default

20 unsuccessful login attempts

50 unsuccessful login attempts

Option

Create a new group for each user

Disable browser's autocomplete feature for username and password fields

Description

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*

Use to deactivate the autocomplete in the log-in box. The autocomplete features can be optionally set in the userâ€™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.

Default

Disabled

Disabled

Option

On permission denied, display login module

Descriptive sentence to ask a user to log in

Prevent multiple log-ins by the same user

Description

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.

If the login module is called on the page and shown to users who are not logged in, this sentence may ask them to enter their credentials (supports wiki syntax)

Users (other than admin) cannot log in simultaneously with multiple browsers.

Default

Enabled

None

Disabled

Option

Clean expired cookies

Grab session if already logged in

Protect all sessions with HTTPS

Description

Automatically clean expired cookies from the database when anyone logs in.

If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out

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*

Default

Enabled

Disabled

Disabled

Option

Use HTTPS login

Description

Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.

⚠ *Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible*

⁝☰ Disabled | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login

Default

Allow secure (HTTPS) login

Option
HTTP Basic Authentication
Users can choose to stay in SSL mode after an HTTPS login
Users can switch between secured or standard mode at login
HTTP port

Description

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

☰ Disable | SSL Only (Recommended) | Always

The port used to access this server; if not specified, port %0 will be used

👆 *If not specified, port %0 will be used*

Default

Disable

Disabled

Disabled

None

Option

HTTPS port

HTTPS for user-specific links

Remember me

Description

the HTTPS port for this server.

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.

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

Disabled | User's choice | Always

Default

443

Disabled

User's choice

Option	
Duration	
Refresh the remember-me cookie expiration	
Cookie name	
Domain	

Description

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

:list: 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 8 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year

Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.

Name of the cookie to remember the user's login

:point_up: *Changing the cookie name forces an instant logout for all user sessions. Including yours.*

The domain that the cookie is available to.

Default

1 month

Enabled

Tikiwiki

None

Option

Path

Cookie Consent

Cookie consent name

Description

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*

Ask permission of the user before setting any cookies, and comply with the response.
👆 *Complies with EU Privacy and Electronic Communications Regulations.* ⚗️

Name of the cookie to record the user's consent if the user agrees. ⚗️

Default

/

Disabled

Tiki_cookies_accepted

Option

Cookie consent expiration

Cookie consent text

Cookie consent question

Description

Expiration date of the cookie to record consent (in days). 🧪

Description for the dialog.
👆 *Wiki-parsed* 🧪

Specific question next to the checkbox for agreement. Leave empty to not display a checkbox.
👆 *Wiki-parsed* 🧪

Default

365 days

privacy notice.">This website would like to ...

I accept cookies from this ...

Option

Cookie consent for analytics

Cookie consent alert

Cookie consent button

Description

Make it possible for users to opt in to essential cookies, such as "remember login", "timezone" etc without opting in to third party cookies such as those for Google Analytics and other external services.
👆 *Makes the checkbox opt in to accept "non-essential" cookies* ⚗️

Alert displayed when user tries to access or use a feature requiring cookies. ⚗️

Label on the agreement button. ⚗️

Default

Disabled

Sorry, cookie consent required

Continue

Option

Cookie consent display mode

Cookie consent dialog ID

Cookie consent disabled

Banning system

Ban usernames and emails

Description

Appearance of consent dialog

Plain | Banner | Dialog

DOM id for the dialog container div.

Do not give the option to refuse cookies but still inform the user about cookie usage.

Deny access to specific users based on username, IP, and date/time range.

Banning rules use both email and username to match rules.

Default

None

Cookie_consent_div

Disabled

Disabled

Disabled

Option

Attempts number

Banning system

Use email as username

Description

Number of attempts user is allowed to login incorrectly before banning them from further attempts.

The duration of the incorrect login attempts ban in minutes.

Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.

Default

5

30

Disabled

Option

Obscure email when using email as username

User emails must be unique

Show emails validation

User can login via username or email.

Description

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*

The email address of each user must be unique.

Show if an email is already in use on the registration form. Will confirm an email is registered here if so without completing the form.

This will allow users to login using their email (as well as their username).

Default

Disabled

Disabled

Enabled

Disabled

Option

Minimum length

Maximum length

Force lowercase

Description

The least possible number of characters for a valid username.

The greatest number of characters for a valid username.

Automatically convert all alphabetic characters in the username to lowercase letters. For example **JohnDoe** becomes **johndoe**.

Default

1 characters

50 characters

Disabled

Option

Username pattern

Auto-generate 6-digit username on registration

Description

This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /'\-_a-zA-Z0-9@\.Ã—-Ã—Âª*$/ or, for Chinese, use: /'\-_a-zA-Z0-9@\.\x00-\xff*$/

This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).

Default

/
'\-_a-zA-Z0-9@\.*$/

Disabled

Option

Forgot password

Allow users to use 2FA

Users can change their password

Description

Users can request a password reset. They will receive a link by email.

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

Allow users to enable Two-factor Authentication.

Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.

Default

Enabled

Disabled

Enabled

Option

Require characters and numerals

Require alphabetical characters in lower and upper case

Require special characters

Description

For improved security, require users to include a mix of alphabetical characters and numerals in passwords.

Password must contain at least one lowercase alphabetical character like "a" and one uppercase character like "A". Use this option to require users to select stronger passwords.

Password must contain at least one special character in lower case like **" / $ % ? & * ( ) _ + .** Use this option to require users to select stronger passwords.

Default

Disabled

Disabled

Disabled

Option

Require no consecutive repetition of the same character

Prevent common passwords

The password must be different from the user's log-in name

Minimum length

Description

Password must not contain a consecutive repetition of the same character such as "111" or "aab".

For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.

The least possible number of characters for a valid password.

Default

Disabled

Disabled

Enabled

5 characters

Option

Password expires after

Description

The number of days after which a password will expire. Days are counted starting with the userâ€™s first login. When the password expires, users will be required to select a new password when logging in.

👆 *Use "-1" for never*

Default

-1 days

Unable to load the jQuery Sortable Tables feature.

Option

Authentication method

Intertiki

Users can register

Description

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

Allows several Tiki sites (slaves) to get authentication from a master Tiki site

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.

Default

Tiki

Disabled

Disabled

Option

Validate new user registrations by email

Description

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.

Default

Enabled

Option

Validate user's email server

Require validation by Admin

Description

Tiki will attempt to validate the userâ€™s email address by examining the syntax of the email address. It must be a string of letters, or digits or _ or . or - follows by a @ follows by a string of letters, or digits or _ or . or -. Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.

☰ No | Yes | Yes, with "deep MX" search

The administrator will receive an email for each new user registration, and must validate the user before the user can log in.

Default

No

Disabled

Option

Validator emails (separated by comma) if different than the sender email

Require passcode to register

Passcode

Description

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.

👆 *Alphanumeric code required to complete the registration*

Default

None

Disabled

None

Option

Show passcode on registration form

Registration page key

Description

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.

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).*

Default

Disabled

None

Option

Generate password

Registration referrer check

Display Disposable Emails

Description

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.*

Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)

Show if a user's email address is from a disposable / temporary email address provider

Default

Disabled

Enabled

Disabled

Option

Anonymous editors must enter anti-bot code (CAPTCHA)

CAPTCHA image word length

CAPTCHA image width

CAPTCHA image noise

Description

Use CAPTCHA to ensure that anonymous input is from a person.

Number of characters the CAPTCHA will display.

Width of the CAPTCHA image in pixels.

Level of noise of the CAPTCHA image.
👆 *Choose a smaller number for less noise and easier reading.*

Default

Enabled

6 characters

180 pixels

100

Option

Use reCAPTCHA

Site key

Secret key

reCAPTCHA theme

Version

Description

Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA

👆 *You will need to register at*

http://www.google.com/recaptcha

reCAPTCHA public key obtained after registering.

reCAPTCHA private key obtained after registering.

Choose a theme for the reCAPTCHA widget.

☰ Clean | Black Glass | Red | White

reCAPTCHA version.

☰ 1.0 | 2.0 | 3.0

Default

Disabled

None

None

Clean

2.0

Option

CAPTCHA questions

CAPTCHA questions and answers

Users must choose a group at registration

Description

Requires anonymous visitors to enter the answer to a question.

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*

Users cannot register without choosing one of the groups indicated above.

Default

Disabled

None

Disabled

Option

URL the user is redirected to after account validation

Use a tracker to collect more user information

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.*

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.*

Default

None

Disabled

Option

Present different input fields in the User Wizard than are in the Registration form

Tracker fields presented in the User Wizard as User Details

Use pretty trackers for registration form

Registration pretty tracker template

Description

Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form

User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)

Allows a site manager to design forms using registration fields and have the results of each field displayed in customizable way on a Wiki page or Smarty template.

Use a wiki page name or Smarty template file with a .tpl extension.

Default

Disabled

None

Disabled

None

Option

Hide Mandatory

Output the registration results

Output registration pretty tracker template

Page name field ID

User tracker IDs to sync prefs from

Description

Hide mandatory fields indication with an asterisk (shown by default).

Use a wiki page as template to output the registration results to

Wiki page only

User the tracker's field ID whose value is used as the output page name.

Select one or more trackers to sync user preferences from.

Default

Disabled

Disabled

None

None

None

Option

Tracker field IDs to sync the "real name" pref from

Tracker field IDs to sync user groups

Synchronize long/lat/zoom to location field

Change user system language when changing user tracker item language

Description

Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using "+", for example "2+3,4".

Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.

Synchronize user geolocation preferences with the main location field.

Default

None

None

Disabled

Disabled

Option

Assign a user tracker item when registering if email equals this field

Force users to upload an avatar.

Require users to fill in tracker information

Tracker ID of tracker required to be filled in

Description

Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.

Require users to fill in a tracker form if not done already by prompting them with a modal dialog.

A tracker for articles must contain an "Articles" field

Default

None

Disabled

Disabled

None

Option

Mandatory tracker field to check for required filling in

Fields that are asked for in the modal for force-filling

Use tracker to collect more group information

Description

The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.

Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested

👆 *Go to Admin Groups to select which tracker and fields to display.*

Default

None

None

Disabled

Option

Re-validate user email after

Re-validate user by email after

Description

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 userâ€™s email is still valid.

👆 *Use "-1" for never*

After a certain number of consecutive unsuccessful log-in attempts, the user will receive an email with instruction to validate his or her account. However, the user can still log in with the old password.

👆 *Use "-1" for never*

Default

-1 days

20 unsuccessful login attempts

Option

Suspend account after

Create a new group for each user

Description

After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin must revalidate the account before the user can use it again.

👆 *Use "-1" for never*

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*

Default

50 unsuccessful login attempts

Disabled

Option

Disable browser's autocomplete feature for username and password fields

On permission denied, display login module

Description

Use to deactivate the autocomplete in the log-in box. The autocomplete features can be optionally set in the userâ€™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.

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.

Default

Disabled

Disabled

Option

Descriptive sentence to ask a user to log in

Prevent multiple log-ins by the same user

Clean expired cookies

Grab session if already logged in

Description

If the login module is called on the page and shown to users who are not logged in, this sentence may ask them to enter their credentials (supports wiki syntax)

Users (other than admin) cannot log in simultaneously with multiple browsers.

Automatically clean expired cookies from the database when anyone logs in.

If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out

Default

None

Disabled

Enabled

Disabled

Option

Protect all sessions with HTTPS

Description

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*

Default

Disabled

Option

Use HTTPS login

Description

Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.

⚠ *Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible*

⁝☰ Disabled | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login

Default

Allow secure (HTTPS) login

Option
HTTP Basic Authentication
Users can choose to stay in SSL mode after an HTTPS login
Users can switch between secured or standard mode at login
HTTP port

Description

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

☰ Disable | SSL Only (Recommended) | Always

The port used to access this server; if not specified, port %0 will be used

👆 *If not specified, port %0 will be used*

Default

Disable

Enabled

Disabled

None

Option

HTTPS port

HTTPS for user-specific links

Remember me

Description

the HTTPS port for this server.

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.

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

Disabled | User's choice | Always

Default

443

Disabled

Disabled

Option	
Duration	
Refresh the remember-me cookie expiration	
Cookie name	
Domain	

Description

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

:list: 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 8 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year

Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.

Name of the cookie to remember the user's login

:point_up: *Changing the cookie name forces an instant logout for all user sessions. Including yours.*

The domain that the cookie is available to.

Default

2 hours

Disabled

Tikiwiki

None

Option

Path

Cookie Consent

Cookie consent name

Description

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*

Ask permission of the user before setting any cookies, and comply with the response.
👆 *Complies with EU Privacy and Electronic Communications Regulations.* ⚗️

Name of the cookie to record the user's consent if the user agrees. ⚗️

Default

/

Disabled

Tiki_cookies_accepted

Option

Cookie consent expiration

Cookie consent text

Cookie consent question

Description

Expiration date of the cookie to record consent (in days). 🧪

Description for the dialog.
👆 *Wiki-parsed* 🧪

Specific question next to the checkbox for agreement. Leave empty to not display a checkbox.
👆 *Wiki-parsed* 🧪

Default

365 days

privacy notice.">This website would like to ...

I accept cookies from this ...

Option

Cookie consent for analytics

Cookie consent alert

Cookie consent button

Description

Make it possible for users to opt in to essential cookies, such as "remember login", "timezone" etc without opting in to third party cookies such as those for Google Analytics and other external services.
👆 *Makes the checkbox opt in to accept "non-essential" cookies* ⚗️

Alert displayed when user tries to access or use a feature requiring cookies. ⚗️

Label on the agreement button. ⚗️

Default

Disabled

Sorry, cookie consent required

Continue

Option

Cookie consent display mode

Cookie consent dialog ID

Cookie consent disabled

Banning system

Ban usernames and emails

Description

Appearance of consent dialog

Plain | Banner | Dialog

DOM id for the dialog container div.

Do not give the option to refuse cookies but still inform the user about cookie usage.

Deny access to specific users based on username, IP, and date/time range.

Banning rules use both email and username to match rules.

Default

None

Cookie_consent_div

Disabled

Disabled

Disabled

Option

Attempts number

Banning system

Use email as username

Description

Number of attempts user is allowed to login incorrectly before banning them from further attempts.

The duration of the incorrect login attempts ban in minutes.

Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.

Default

5

30

Disabled

Option

Obscure email when using email as username

User emails must be unique

Show emails validation

User can login via username or email.

Description

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*

The email address of each user must be unique.

Show if an email is already in use on the registration form. Will confirm an email is registered here if so without completing the form.

This will allow users to login using their email (as well as their username).

Default

Disabled

Disabled

Enabled

Disabled

Option

Minimum length

Maximum length

Force lowercase

Description

The least possible number of characters for a valid username.

The greatest number of characters for a valid username.

Automatically convert all alphabetic characters in the username to lowercase letters. For example **JohnDoe** becomes **johndoe**.

Default

1 characters

50 characters

Disabled

Option

Username pattern

Auto-generate 6-digit username on registration

Description

This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /'\-_a-zA-Z0-9@\.Ã—-Ã—Âª*$/ or, for Chinese, use: /'\-_a-zA-Z0-9@\.\x00-\xff*$/

This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).

Default

/'\-_a-zA-Z0-9@\.*$/

Disabled

Option

Forgot password

Allow users to use 2FA

Users can change their password

Description

Users can request a password reset. They will receive a link by email.

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

Allow users to enable Two-factor Authentication.

Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.

Default

Enabled

Disabled

Enabled

Option

Require characters and numerals

Require alphabetical characters in lower and upper case

Require special characters

Description

For improved security, require users to include a mix of alphabetical characters and numerals in passwords.

Password must contain at least one lowercase alphabetical character like "a" and one uppercase character like "A". Use this option to require users to select stronger passwords.

Password must contain at least one special character in lower case like **" / $ % ? & * ( ) _ + .** Use this option to require users to select stronger passwords.

Default

Disabled

Disabled

Disabled

Option

Require no consecutive repetition of the same character

Prevent common passwords

The password must be different from the user's log-in name

Minimum length

Description

Password must not contain a consecutive repetition of the same character such as "111" or "aab".

For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.

The least possible number of characters for a valid password.

Default

Disabled

Disabled

Enabled

5 characters

Option

Password expires after

Description

The number of days after which a password will expire. Days are counted starting with the userâ€™s first login. When the password expires, users will be required to select a new password when logging in.

👆 *Use "-1" for never*

Default

-1 days

Unable to load the jQuery Sortable Tables feature.

Option

Authentication method

Intertiki

Users can register

Description

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

Allows several Tiki sites (slaves) to get authentication from a master Tiki site

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.

Default

Tiki

Disabled

Disabled

Option

Validate new user registrations by email

Description

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.

Default

Enabled

Option

Validate user's email server

Require validation by Admin

Description

Tiki will attempt to validate the userâ€™s email address by examining the syntax of the email address. It must be a string of letters, or digits or _ or . or - follows by a @ follows by a string of letters, or digits or _ or . or -. Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.

☰ No | Yes | Yes, with "deep MX" search

The administrator will receive an email for each new user registration, and must validate the user before the user can log in.

Default

No

Disabled

Option

Validator emails (separated by comma) if different than the sender email

Require passcode to register

Passcode

Description

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.

👆 *Alphanumeric code required to complete the registration*

Default

None

Disabled

None

Option

Show passcode on registration form

Registration page key

Description

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.

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).*

Default

Disabled

None

Option

Generate password

Registration referrer check

Anonymous editors must enter anti-bot code (CAPTCHA)

CAPTCHA image word length

Description

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.*

Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)

Use CAPTCHA to ensure that anonymous input is from a person.

Number of characters the CAPTCHA will display.

Default

Disabled

Enabled

Enabled

6 characters

Option

CAPTCHA image width

CAPTCHA image noise

Use reCAPTCHA

Site key

Secret key

Description

Width of the CAPTCHA image in pixels.

Level of noise of the CAPTCHA image.
👆 *Choose a smaller number for less noise and easier reading.*

Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA
👆 *You will need to register at http://www.google.com/recaptcha*

reCAPTCHA public key obtained after registering.

reCAPTCHA private key obtained after registering.

Default

180 pixels

100

Disabled

None

None

Option

reCAPTCHA theme

Version

CAPTCHA questions

Description

Choose a theme for the reCAPTCHA widget.

- Clean | Black Glass | Red | White

reCAPTCHA version.

- 1.0 | 2.0 | 3.0

Requires anonymous visitors to enter the answer to a question.

Default

Clean

2.0

Disabled

Option

CAPTCHA questions and answers

Users must choose a group at registration

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*

Users cannot register without choosing one of the groups indicated above.

Default

None

Disabled

Option

URL the user is redirected to after account validation

Use a tracker to collect more user information

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.*

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.*

Default

None

Disabled

Option

Present different input fields in the User Wizard than are in the Registration form

Tracker fields presented in the User Wizard as User Details

Use pretty trackers for registration form

Registration pretty tracker template

Description

Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form

User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)

Allows a site manager to design forms using registration fields and have the results of each field displayed in customizable way on a Wiki page or Smarty template.

Use a wiki page name or Smarty template file with a .tpl extension.

Default

Disabled

None

Disabled

None

Option

Hide Mandatory

Output the registration results

Output registration pretty tracker template

Page name field ID

User tracker IDs to sync prefs from

Description

Hide mandatory fields indication with an asterisk (shown by default).

Use a wiki page as template to output the registration results to

Wiki page only

User the tracker's field ID whose value is used as the output page name.

Select one or more trackers to sync user preferences from.

Default

Disabled

Disabled

None

None

None

Option

Tracker field IDs to sync the "real name" pref from

Tracker field IDs to sync user groups

Synchronize long/lat/zoom to location field

Change user system language when changing user tracker item language

Description

Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using "+", for example "2+3,4".

Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.

Synchronize user geolocation preferences with the main location field.

Default

None

None

Disabled

Disabled

Option

Assign a user tracker item when registering if email equals this field

Force users to upload an avatar.

Require users to fill in tracker information

Tracker ID of tracker required to be filled in

Description

Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.

Require users to fill in a tracker form if not done already by prompting them with a modal dialog.

A tracker for articles must contain an "Articles" field

Default

None

Disabled

Disabled

None

Option

Mandatory tracker field to check for required filling in

Fields that are asked for in the modal for force-filling

Use tracker to collect more group information

Description

The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.

Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested

👆 *Go to Admin Groups to select which tracker and fields to display.*

Default

None

None

Disabled

Option

Re-validate user email after

Re-validate user by email after

Description

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 userâ€™s email is still valid.

👆 *Use "-1" for never*

After a certain number of consecutive unsuccessful log-in attempts, the user will receive an email with instruction to validate his or her account. However, the user can still log in with the old password.

👆 *Use "-1" for never*

Default

-1 days

20 unsuccessful login attempts

Option

Suspend account after

Create a new group for each user

Description

After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin must revalidate the account before the user can use it again.

👆 *Use "-1" for never*

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*

Default

50 unsuccessful login attempts

Disabled

Option

Disable browser's autocomplete feature for username and password fields

On permission denied, display login module

Description

Use to deactivate the autocomplete in the log-in box. The autocomplete features can be optionally set in the userâ€™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.

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.

Default

Disabled

Disabled

Option

Prevent multiple log-ins by the same user

Clean expired cookies

Grab session if already logged in

Description

Users (other than admin) cannot log in simultaneously with multiple browsers.

Automatically clean expired cookies from the database when anyone logs in.

If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out

Default

Disabled

Enabled

Disabled

Option

Protect all sessions with HTTPS

Description

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*

Default

Disabled

Option

Use HTTPS login

Description

Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.

⚠ *Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible*

⁝☰ Disabled | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login

Default

Allow secure (HTTPS) login

Option
HTTP Basic Authentication
Users can choose to stay in SSL mode after an HTTPS login
Users can switch between secured or standard mode at login
HTTP port

Description

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

☰ Disable | SSL Only (Recommended) | Always

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

👆 *If not specified, port 80 will be used*

Default

Disable

Enabled

Disabled

None

Option

HTTPS port

HTTPS for user-specific links

Remember me

Description

the HTTPS port for this server.

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.

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

Disabled | User's choice | Always

Default

443

Disabled

Disabled

Option	
Duration	
Refresh the remember-me cookie expiration	
Cookie name	
Domain	

Description

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

:list: 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 8 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year

Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.

Name of the cookie to remember the user's login

:point_up: *Changing the cookie name forces an instant logout for all user sessions. Including yours.*

The domain that the cookie is available to.

Default

2 hours

Disabled

Tikiwiki

None

Option

Path

Cookie Consent

Cookie consent name

Description

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*

Ask permission of the user before setting any cookies, and comply with the response.
👆 *Complies with EU Privacy and Electronic Communications Regulations.* ⚗️

Name of the cookie to record the user's consent if the user agrees. ⚗️

Default

/wikisuite/24.x/tiki/

Disabled

Tiki_cookies_accepted

Option

Cookie consent expiration

Cookie consent text

Cookie consent question

Description

Expiration date of the cookie to record consent (in days). 🧪

Description for the dialog.
👆 *Wiki-parsed* 🧪

Specific question next to the checkbox for agreement. Leave empty to not display a checkbox.
👆 *Wiki-parsed* 🧪

Default

365 days

privacy notice.">This website would like to ...

I accept cookies from this ...

Option

Cookie consent for analytics

Cookie consent alert

Cookie consent button

Description

Make it possible for users to opt in to essential cookies, such as "remember login", "timezone" etc without opting in to third party cookies such as those for Google Analytics and other external services.
👆 *Makes the checkbox opt in to accept "non-essential" cookies* ⚗️

Alert displayed when user tries to access or use a feature requiring cookies. ⚗️

Label on the agreement button. ⚗️

Default

Disabled

Sorry, cookie consent required

Continue

Option

Cookie consent display mode

Cookie consent dialog ID

Cookie consent disabled

Banning system

Ban usernames and emails

Description

Appearance of consent dialog

Plain | Banner | Dialog

DOM id for the dialog container div.

Do not give the option to refuse cookies but still inform the user about cookie usage.

Deny access to specific users based on username, IP, and date/time range.

Banning rules use both email and username to match rules.

Default

None

Cookie_consent_div

Disabled

Disabled

Disabled

Option

Use email as username

Obscure email when using email as username

User emails must be unique

User can login via username or email.

Description

Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.

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*

The email address of each user must be unique.

This will allow users to login using their email (as well as their username).

Default

Disabled

Disabled

Disabled

Disabled

Option

Minimum length

Maximum length

Force lowercase

Description

The least possible number of characters for a valid username.

The greatest number of characters for a valid username.

Automatically convert all alphabetic characters in the username to lowercase letters. For example **JohnDoe** becomes **johndoe**.

Default

1 characters

50 characters

Disabled

Option

Username pattern

Auto-generate 6-digit username on registration

Description

This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /'\-_a-zA-Z0-9@\.Ã—-Ã—Âª*$/ or, for Chinese, use: /'\-_a-zA-Z0-9@\.\x00-\xff*$/

This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).

Default

/
'\-_a-zA-Z0-9@\.*$/

Disabled

Option

Forgot password

Allow users to use 2FA

Users can change their password

Description

Users can request a password reset. They will receive a link by email.

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

Allow users to enable Two-factor Authentication.

Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.

Default

Enabled

Disabled

Enabled

Option

Require characters and numerals

Require alphabetical characters in lower and upper case

Require special characters

Description

For improved security, require users to include a mix of alphabetical characters and numerals in passwords.

Password must contain at least one lowercase alphabetical character like "a" and one uppercase character like "A". Use this option to require users to select stronger passwords.

Password must contain at least one special character in lower case like **" / $ % ? & * ( ) _ + .** Use this option to require users to select stronger passwords.

Default

Disabled

Disabled

Disabled

Option

Require no consecutive repetition of the same character

Prevent common passwords

The password must be different from the user's log-in name

Minimum length

Description

Password must not contain a consecutive repetition of the same character such as "111" or "aab".

For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.

The least possible number of characters for a valid password.

Default

Disabled

Disabled

Enabled

5 characters

Option

Password expires after

Description

The number of days after which a password will expire. Days are counted starting with the userâ€™s first login. When the password expires, users will be required to select a new password when logging in.

👆 *Use "-1" for never*

Default

-1 days

Unable to load the jQuery Sortable Tables feature.

Option

Authentication method

Description

Tiki supports several authentication methods. The default method is to use the internal user database.

Tiki | Tiki and OpenID | Tiki and PAM | CAS (Central Authentication Service) | Shibboleth | Web Server | phpBB

Default

Tiki

Option

Intertiki

Users can register

Validate new user registrations by email

Description

Allows several Tiki sites (slaves) to get authentication from a master Tiki site

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.

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.

Default

Disabled

Disabled

Enabled

Option

Validate user's email server

Require validation by Admin

Description

Tiki will attempt to validate the userâ€™s email address by examining the syntax of the email address. It must be a string of letters, or digits or _ or . or - follows by a @ follows by a string of letters, or digits or _ or . or -. Tiki will perform a DNS lookup and attempt to open a SMTP session to validate the email server.

☰ No | Yes | Yes, with "deep MX" search

The administrator will receive an email for each new user registration, and must validate the user before the user can log in.

Default

No

Disabled

Option

Validator emails (separated by comma) if different than the sender email

Require passcode to register

Passcode

Description

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.

👆 *Alphanumeric code required to complete the registration*

Default

None

Disabled

None

Option

Show passcode on registration form

Registration page key

Description

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.

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).*

Default

Disabled

None

Option

Generate password

Registration referrer check

Anonymous editors must enter anti-bot code (CAPTCHA)

CAPTCHA image word length

Description

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.*

Use the HTTP referrer to check registration POST is sent from same host. (May not work on some setups.)

Use CAPTCHA to ensure that anonymous input is from a person.

Number of characters the CAPTCHA will display.

Default

Disabled

Enabled

Enabled

6 characters

Option

CAPTCHA image width

CAPTCHA image noise

Use reCAPTCHA

Site key

Secret key

Description

Width of the CAPTCHA image in pixels.

Level of noise of the CAPTCHA image.
👆 *Choose a smaller number for less noise and easier reading.*

Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA
👆 *You will need to register at http://www.google.com/recaptcha*

reCAPTCHA public key obtained after registering.

reCAPTCHA private key obtained after registering.

Default

180 pixels

100

Disabled

None

None

Option

reCAPTCHA theme

Version

CAPTCHA questions

Description

Choose a theme for the reCAPTCHA widget.

- Clean | Black Glass | Red | White

reCAPTCHA version.

- 1.0 | 2.0 | 3.0

Requires anonymous visitors to enter the answer to a question.

Default

Clean

2.0

Disabled

Option

CAPTCHA questions and answers

Users must choose a group at registration

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*

Users cannot register without choosing one of the groups indicated above.

Default

None

Disabled

Option

URL the user is redirected to after account validation

Use a tracker to collect more user information

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.*

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.*

Default

None

Disabled

Option

Present different input fields in the User Wizard than are in the Registration form

Tracker fields presented in the User Wizard as User Details

Use pretty trackers for registration form

Registration pretty tracker template

Hide Mandatory

Description

Ask a different set of fields for the User Details section in the User Wizard than the ones shown in the Registration form

User's information tracker fields presented in the User Wizard as User Details (separate field IDs with colons)

Use pretty trackers for registration form

Use a wiki page name or Smarty template file with a .tpl extension.

Hide mandatory fields indication with an asterisk (shown by default).

Default

Disabled

None

Disabled

None

Disabled

Option

Output the registration results

Output registration pretty tracker template

Page name field ID

User tracker IDs to sync prefs from

Tracker field IDs to sync the "real name" pref from

Description

Use a wiki page as template to output the registration results to

Wiki page only

User the tracker's field ID whose value is used as the output page name.

Select one or more trackers to sync user preferences from.

Enter the comma-separated IDs in order of priority to be chosen; each item can concatenate multiple fields using "+", for example "2+3,4".

Default

Disabled

None

None

None

None

Option
Tracker field IDs to sync user groups
Synchronize long/lat/zoom to location field
Change user system language when changing user tracker item language
Assign a user tracker item when registering if email equals this field

Description

Enter the comma-separated IDs of all fields that contain group names to which to sync user groups.

Synchronize user geolocation preferences with the main location field.

Default

None

Disabled

Disabled

None

Option

Force users to upload an avatar.

Require users to fill in tracker information

Tracker ID of tracker required to be filled in

Mandatory tracker field to check for required filling in

Description

Require the user to upload a profile picture if they haven't done so already by prompting them with a modal popup.

Require users to fill in a tracker form if not done already by prompting them with a modal dialog.

A tracker for articles must contain an "Articles" field

The permname of field that is checked to see if user has completed the form. If field is empty, user has not completed it.

Default

Disabled

Disabled

None

None

Option

Fields that are asked for in the modal for force-filling

Use tracker to collect more group information

Re-validate user email after

Description

Comma-separated permanent names of fields that are requested in the modal for required filling in. If empty, all fields are requested

👆 *Go to Admin Groups to select which tracker and fields to display.*

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 userâ€™s email is still valid.

👆 *Use "-1" for never*

Default

None

Disabled

-1 days

Option

Re-validate user by email after

Suspend account after

Description

After a certain number of consecutive unsuccessful log-in attempts, the user will receive an email with instruction to validate his or her account. However, the user can still log in with the old password.

👆 *Use "-1" for never*

After a certain number of consecutive unsuccessful login attempts, the account is suspended. An admin must revalidate the account before the user can use it again.

👆 *Use "-1" for never*

Default

20 unsuccessful login attempts

50 unsuccessful login attempts

Option

Create a new group for each user

Disable browser's autocomplete feature for username and password fields

Description

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*

Use to deactivate the autocomplete in the log-in box. The autocomplete features can be optionally set in the userâ€™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.

Default

Disabled

Disabled

Option

On permission denied, display login module

Prevent multiple log-ins by the same user

Grab session if already logged in

Description

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.

Users (other than admin) cannot log in simultaneously with multiple browsers.

If users are blocked from logging in simultaneously, grab the session. Will force existing user to be logged out

Default

Disabled

Disabled

Disabled

Option

Protect all sessions with HTTPS

Description

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*

Default

Disabled

Option

Use HTTPS login

Description

Increase security by allowing to transmit authentication credentials over SSL. Certificates must be configured on the server.

⚠ *Do not require HTTPS until the connection has been set up and tested; otherwise, the website will be inaccessible*

⁝☰ Disabled | Allow secure (HTTPS) login | Encourage secure (HTTPS) login | Consider we are always in HTTPS, but do not check | Require secure (HTTPS) login

Default

Allow secure (HTTPS) login

Option
HTTP Basic Authentication
Users can choose to stay in SSL mode after an HTTPS login
Users can switch between secured or standard mode at login
HTTP port

Description

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

☰ Disable | SSL Only (Recommended) | Always

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

👆 *If not specified, port 80 will be used*

Default

Disable

Enabled

Disabled

None

Option

HTTPS port

HTTPS for user-specific links

Remember me

Description

the HTTPS port for this server.

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.

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

Disabled | User's choice | Always

Default

443

Disabled

Disabled

Option	
Duration	
Refresh the remember-me cookie expiration	
Cookie name	
Domain	

Description

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

:list: 5 minutes | 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 8 hours | 10 hours | 20 hours | 1 day | 1 week | 1 month | 1 year

Each time a user is logged in with a cookie set in a previous session, the cookie expiration date is updated.

Name of the cookie to remember the user's login

:point_up: *Changing the cookie name forces an instant logout for all user sessions. Including yours.*

The domain that the cookie is available to.

Default

2 hours

Disabled

Tikiwiki

None

Option

Path

Cookie Consent

Cookie consent name

Description

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*

Ask permission of the user before setting any cookies, and comply with the response.
👆 *Complies with EU Privacy and Electronic Communications Regulations.* ⚗️

Name of the cookie to record the user's consent if the user agrees. ⚗️

Default

/wikisuite/21.x/tiki/

Disabled

Tiki_cookies_accepted

Option

Cookie consent expiration

Cookie consent text

Cookie consent question

Cookie consent alert

Cookie consent button

Description

Expiration date of the cookie to record consent (in days). 🧪

Description for the dialog.
👆 *Wiki-parsed* 🧪

Specific question next to the checkbox for agreement. Leave empty to not display a checkbox.
👆 *Wiki-parsed* 🧪

Alert displayed when user tries to access or use a feature requiring cookies. 🧪

Label on the agreement button. 🧪

Default

365 days

privacy notice.">This website would like to ...

I accept cookies from this ...

Sorry, cookie consent required

Continue

Option

Cookie consent mode

Cookie consent dialog ID

Cookie consent disabled

Banning system

Attempts number

Description

Appearance of consent dialog

Dialog style requires feature_jquery_ui

Plain | Banner | Dialog

DOM id for the dialog container div.

Do not give the option to refuse cookies but still inform the user about cookie usage.

Deny access to specific users based on username, IP, and date/time range.

Number of attempts user is allowed to login incorrectly before banning them from further attempts.

Default

None

Cookie_consent_div

Disabled

Disabled

5

Option

Banning system

Use email as username

Obscure email when using email as username

User emails must be unique

Description

The duration of the incorrect login attempts ban in minutes.

Instead of creating new usernames, use the user's email address for authentication. On the registration form, there will be no Username field.

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*

The email address of each user must be unique.

Default
30
Disabled
Disabled
Disabled

Option

User can login via username or email.

Minimum length

Maximum length

Force lowercase

Description

This will allow users to login using their email (as well as their username).

The least possible number of characters for a valid username.

The greatest number of characters for a valid username.

Automatically convert all alphabetic characters in the username to lowercase letters. For example **JohnDoe** becomes **johndoe**.

Default

Disabled

1 characters

50 characters

Disabled

Option

Username pattern

Auto-generate 6-digit username on registration

Description

This regex pattern requires or forbids the use of certain characters for username. For example, to add Hebrew, use: /'\-_a-zA-Z0-9@\.Ã—-Ã—Âª*$/ or, for Chinese, use: /'\-_a-zA-Z0-9@\.\x00-\xff*$/

This will auto-generate a 6-digit username for users who sign up (they will normally log in with emails only).

Default

/'\-_a-zA-Z0-9@\.*$/

Disabled

Option

Forgot password

Allow users to use 2FA

Users can change their password

Description

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.*

Allow users to enable Two-factor Authentication.

Registered users can change their password from their User Preferences page. If not, passwords can be changed only by the admin.

Default

Enabled

Disabled

Enabled

Option

Require characters and numerals

Require alphabetical characters in lower and upper case

Require special characters

Description

For improved security, require users to include a mix of alphabetical characters and numerals in passwords.

Password must contain at least one lowercase alphabetical character like "a" and one uppercase character like "A". Use this option to require users to select stronger passwords.

Password must contain at least one special character in lower case like **" / $ % ? & * ( ) _ + .** Use this option to require users to select stronger passwords.

Default

Disabled

Disabled

Disabled

Option

Require no consecutive repetition of the same character

Prevent common passwords

The password must be different from the user's log-in name

Minimum length

Description

Password must not contain a consecutive repetition of the same character such as "111" or "aab".

For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.

The least possible number of characters for a valid password.

Default

Disabled

Disabled

Enabled

5 characters

Option

Password expires after

Description

The number of days after which a password will expire. Days are counted starting with the userâ€™s first login. When the password expires, users will be required to select a new password when logging in.

👆 *Use "-1" for never*

Default
-1 days

Unable to load the jQuery Sortable Tables feature.

CUSTOMFIELDS

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

- Home_Phone
- AIM (or other IM handles)
- Address
- Professional_Certs

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

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

The values of the 3 fields are:

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

Limits

1. At this time, there is no web page to create the actual field definitions, you must use the SQL statement shown above.
2. No spaces are allowed in the label, an underscore can be used instead.
3. There is no support for anything other than plain text fields
4. Possible security issue - if a user registers with the name 'CustomFields', they could possibly change the default values, or cause other problems. Possible workaround - create your own user with that name and don't use it for anything.
5. The created fields are informational only, they don't hook into anything useful inside Tiki.

REMEMBER ME

If â€œUserâ€™s Choiceâ€ is selected the Login module will include a â€œRemember meâ€ checkbox.

nWithout 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 â€˜tiki-user-â€™ 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.