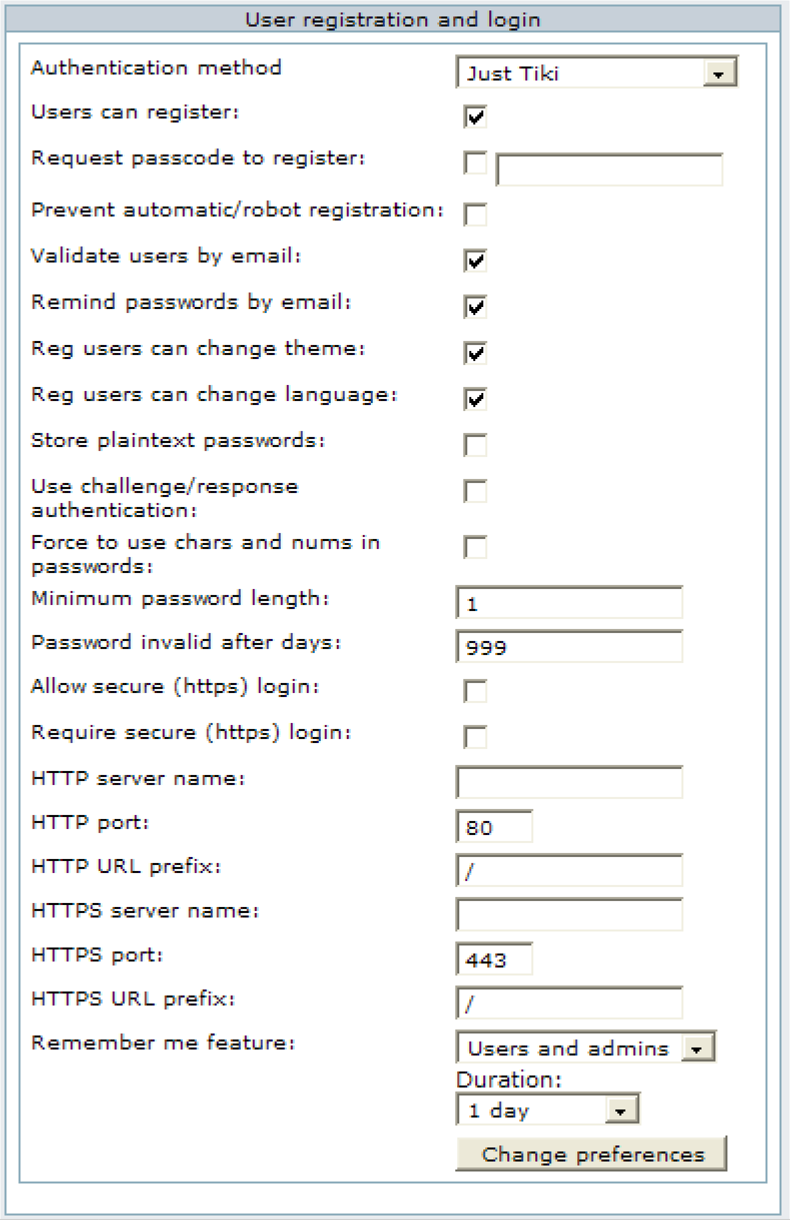
UserRegistrationSettings

Settings Documentation

Clicking the **Login** icon on the **Admin Panel** (see Tiki Config) takes you to the Login settings.

User Registration and Login Settings

In this section of the admin panel you can setup several settings for your user registration and site security features. The settings are the following ones:



User registration and login

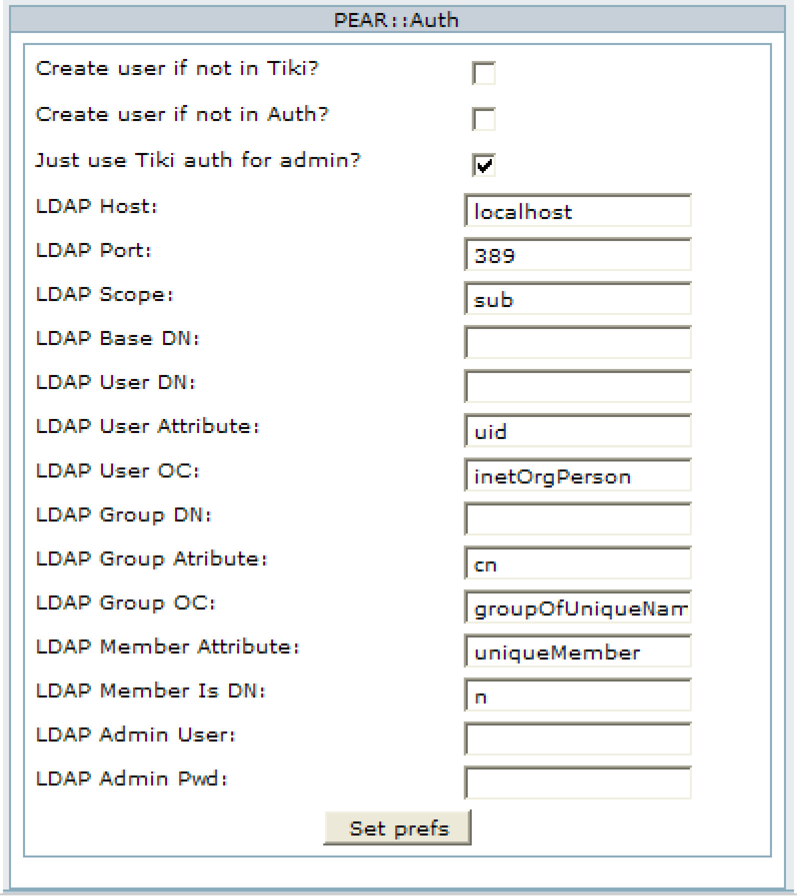
Authentication method: Just Tiki
Users can register: ☑
Request passcode to register: □
Prevent automatic/robot registration: □
Validate users by email: ☑
Remind passwords by email: ☑
Reg users can change theme: ☑
Reg users can change language: ☑
Store plaintext passwords: □
Use challenge/response authentication: □
Force to use chars and nums in passwords: □
Minimum password length: 1
Password invalid after days: 999
Allow secure (https) login: □
Require secure (https) login: □
HTTP server name:
HTTP port: 80
HTTP URL prefix: /
HTTPS server name:
HTTPS port: 443
HTTPS URL prefix: /
Remember me feature: Users and admins
Duration: 1 day

Authentication method	Choose between Tiki, Web server, and Tiki/Pear::Auth. *Tiki* will use your user database built into Tiki. *Web server* will use your web server's authentication. *Tiki/Pear::Auth* is a combination of the Tiki user database and Pear::Auth, which will allow LDAP authentication (and others in future?). See below for Pear settings.
Users can register:	If enabled, the login box will display a **register** link when the user is not logged and the user will have the option to register using a webform. If disabled, each user will need to be setup by an admin.

Request passcode to register:	If enabled, you have to enter a password that will be required to let users register into the system. This can be used in sites where users are *invited* or they receive a passcode after paying a fee or something like that. Semi-private or semi-public sites may enjoy this feature.
Prevent automatic/robot registration:	If enabled, it will present the new user with a graphic showing a series of numbers. They will need to key in these numbers before they will be allowed to register.
Validate users by emails:	If enabled, then when a user registers Tiki will send the user an email with a link that the user must use to login for the first time. Once logged in using this link, the user will be validated and can login as a regular user. This feature is useful if you as an admin want to be sure that the user email addresses are correct and not fake.
Remind passwords by email:	If enabled, then a link to **I forgot my password** will be displayed in the login box. Users will be able to enter their login names, and Tiki will send them emails with their passwords.
Reg users can change theme	If enabled, registered users can configure the theme.
Reg users can change language	If enabled, registered users can configure the site's language.
Store plaintext passwords	If enabled, passwords are stored in the database in clear plaintext; and the remind password feature sends the user his password.
If not enabled, only a hash is stored; and the remind password feature generates a new password and sends that password to the user.	
Use challenge-response authentication	If enabled and the user's browser supports JavaScript, passwords ARE NOT SENT across the network. Instead, a challenge response algorithm is used. Tiki generates a challenge code and the browser sends a response based on the challenge that Tiki verifies to login the user. Challenge responses cannot be reused. This method, if enabled, strongly enforces the security of your user passwords. If you use it you don't need an HTTPs connection for extra security. **The drawback** to this method is that users will have to enter their email address every time they login. - three boxes to fill in not two.
Force to use chars and numbers in passwords	If enabled, Tiki will validate user passwords and reject passwords that do not contain both letters and numbers.
Minimum password length	The minimum length for a password to be accepted.
Passwords are invalid after *n* days	Tiki will force users to change their passwords after this period.
Allow secure https login	Enable this setting If you want to use an HTTPs connection for login.
HTTP and HTTPs settings	Settings for HTTPs logins. You may have your HTTP and HTTPs server in different URLS/ports.
Remember me feature:	If enabled, this will put a **Remember me** checkbox for the user's login. You will also need to set how long the server will remember them.

Pear::Auth settings

Tiki can authenticate users using a LDAP server via Pear::Auth. The following settings only make sense, if you have set "Authentication method" to "Tiki/Pear::Auth" in the above dialog. Tiki then uses the LDAP server in addition to its own user database (users_users) to authenticate users.



PEAR::Auth

Create user if not in Tiki?	□
Create user if not in Auth?	□
Just use Tiki auth for admin?	☑
LDAP Host:	localhost
LDAP Port:	389
LDAP Scope:	sub
LDAP Base DN:	
LDAP User DN:	
LDAP User Attribute:	uid
LDAP User OC:	inetOrgPerson
LDAP Group DN:	
LDAP Group Atribute:	cn
LDAP Group OC:	groupOfUniqueNam
LDAP Member Attribute:	uniqueMember
LDAP Member Is DN:	n
LDAP Admin User:	
LDAP Admin Pwd:	

Create user if not in Tiki?	If a user was authenticated via LDAP, but not found in the Tiki user database, Tiki will create an entry in its user database if this option is checked. **If this option is disabled, this user wouldn't be able to log in**
Create user if not in Auth?	If a user was authenticated by Tiki's user database, but not found on the LDAP server, Tiki will create an LDAP entry for this user. See Pear::Auth on how an entry is created.
Just use tiki auth for admin?	If this option is set, the user "admin" will be authenticated by only using Tiki's user database and not via LDAP. This option has no effect on users other than "admin".
LDAP Host	The hostname or ip address of you LDAP server (usually localhost).
LDAP Port	The port number your LDAP server uses (389 is the default).
LDAP Scope	Search scope (base = Base object search, one = one-level search, sub = Subtree search (default)) used during authentication for finding a user on the LDAP server.
LDAP Base DN	Base DN of the LDAP server. If you leave this empty, Pear::Auth will try to query your LDAP server for its base DN. Example: **dc=my-company,dc=com**
LDAP User DN	RDN to prepend to the base DN when searching for a user. Example: **ou=People** will result search in **ou=People,dc=my-company,dc=com**
LDAP User attribute	Attribute that contains the username.
LDAP User OC	Object class an entry must have when searching for a user. This is mandatory ! If you dont know what to fill in, use * **(an asterix)**
LDAP Admin User	DN of the entry to use to bind to the LDAP server for user creation. While authentication works without binding as a privileged DN, creation of an entry usually does not. This admin DN is only used when creating user entries on the LDAP server (i.e. only if the option **Create user if not in Auth** is checked). Authentication works without an admin DN (Pear::Auth will try to bind using the username/password to authenticate).

LDAP Admin Pwd	Password for the above DN.

The **LDAP Group** and **LDAP Member** settings are currently not used by Tiki (as of 1.8rc2).

TikiTeam

Who is working here generally?

UserPagejbutler
WhiteBoy