Login & External Authentication

Overview of Login Methods

Tiki allows you to use several different login authentication methods. For standalone sites (not connected to a central authentication server), you can use "Just Tiki" or "Web Server". For sites that are part of a larger environment Tiki offers Apache (basic HTTP auth), LDAP (Active Directory), CAS, and Shibboleth authentication.

The installation environment plays a role in determining the authentication method to be used. On a fully accessible server, an administrator has a choice of any/all of the authentication methods listed on this page.

Authentication With Shared Hosting

In a shared hosting environment (FTP access only) the authentication options become severely limited. While it is ossible to setup an OpenID server with FTP access (Community-ID is one such project) it is not well documented. As o 4/09, setting up OpenLDAP, Shibboleth, or CAS are effectively impossible with FTP access only and may be impossible (depending on access rights) with a shell access account.

Just Tiki

The **Just Tiki** authentication method uses the usernames and passwords stored in the Tiki database for authentication
This is best used for sites that are not part of a larger intranet.

Web Server (HTTP)

A common way of protecting webpages is through Basic HTTP authentication. The web server sends a "401 Authentication Required" header when a protected page is requested. The browser would then prompt the user for a username and password. Access is allowed if the username password pair are valid; else, the web server sends a HTTP 401 error, meaning "access denied." HTTP authentication is usually used by creating a .htaccess file. (Only in Apache?) Tiki is able to detect when a visitor to the site is currently logged in using Basic HTTP Authentication. If the username of the user matches a username within Tiki's database, Tiki will automatically log the user in and, of course, grant all the assigned permissions.

Using Web Server authentication can be convenient for a shared hosting installation of Tiki. User management becomes more of a challenge if multiple Tiki's are to be installed. However, in Tiki 3.0 group information and users will still need to be added to each and every sub-Tiki inside the authorized domain.

Options

LDAP (Active Directory)

LDAP authentication

OpenID Connect

OpenID Connect

SAML

- SAML

Hybridauth Social Sign On Library

- Hybridauth social login supports dozens of providers: https://hybridauth.github.io/providers.html

IMAP

IMAP Authentication

POP3

POP3 Authentication

Vpopmail

Vpopmail Authentication

Tiki and Pam

PAM authentication

CAS

CAS Authentication

Shibboleth

Shibboleth Authentication

phpBB

phpBB Authentication

Future Plans (please help!)

- CACert (or other) Client Certificates
- GPG/PGP PKI, including tools such as WebPG
- Post-Login Security Question? Like when logging into a bank website.

Future Delusions

- YubiKey or, egads, YubiHSM!
- Apache TripleSec

Deprecated

OpenID

- OpenID

alias

- Login Authentication Methods
- Login Authentication Method