PAM Authentication tab

Related Topics

- External Authentication

Overview
Tiki can authenticate users using a PAM server

To Access
From the Login Admin page, click the **PAM** tab.

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database.	Disabled
Use Tiki authentication for Admin log-in	The user “admin” will be authenticated by **only** using Tiki’s user database. This option has no effect on users other than “admin”.	Disabled

AuthPAM

AuthPAM provides PAM authentication to Tikiwiki just as Pear Auth does with LDAP.
It's mainly intended for those tiki admins who have integrated their Linux boxes onto their network's authentication using PAM; For example, admins might have their Linux boxes authenticate through PAM to their Windows 2000 Active Directory Domain (via winbind and kerberos 5) so with AuthPAM
then, they can authenticate their networked users against tiki without adding them by hand

Admin Documentation

AuthPAMOld configuration is very simple once you've met all the requirements (only a few). Once met you just have to go to the Login section of TikiAdmin.
There will be a nice option onto 'Method' called 'Tiki and PAM' (which you should select if you plan to use it!).

Requirements for AuthPAM

AuthPAMOld has a small requirement that must be met in order to work; you need pam_auth php module. I've seen it's on some Linux distributions but not on all.
On the main page AuthPAM Link's section you can get the link to the author's home to get the module and compile it if your distribution doesn't include a binary package.

After compiling and installing the module as stated in its documentation you have to create a PAM service for Tiki (normally at /etc/pam.d).

Then just jump onto Tikiwiki and setup PAM there.

Permissions!

Take care of file permissions; remember that php runs with apache privileges, normally a normal user account like www-data or so. If you plan to use PAM against your system's users and your system uses shadowed password you should remember that /etc/shadow is only readable by root, so php won't be able to read it
(the PAM library runs with the calling user privileges), so you'll have to workaround it, maybe letting your web server's user read shadow file or so.

Security Issues

With a default PAM service any account will be granted (try user: nobody) so here are a few things to take care about that:

It is recommended that you make use of pam_require module to require a specific group to be in for the user. Also you can take a look at PAM Modules at kernel.org to refine a bit more your pam service for tiki.

Also take note that pam only receives a user/pass pair and checks it; it relays on your web server settings to handle a secure transaction of that pair from the browser to the server. SSL is recommended.