

User Encryption

User encryption aims to provide secure, personal storage of sensitive data, e.g. external usernames and passwords

About User Encryption

When linking multiple systems together, it is often required to have a username and a password for the target system available, in order to login. The other system can be an external database, a web service, etc.

User Encryption enables secure storage of such external log-in credentials. The decryption key is **not** stored by Tiki, and it is only available when the user is logged in.

Notes:

- This is a new an experimental feature in Tiki 13 and has been backported for Tiki 12.2, so it is available (as experimental) in the LTS version
- Use the Domain Password module to allow the user to specify username and password
- CryptLib must be integrated by coding to access the domain. CryptLib provides the decrypted domain credentials

See also User Encryption.

Password Domains

Each linked system makes up a "password domain". Multiple users can log in to a domain. A password domain has a name. The name must be unique.

The interface to a linked system, uses the password domain name to look-up a user's credentials for the system.

The module "Domain Password", prompts the user for a password.

The password is encrypted and saved associated with the domain specified in the module.




Configuring Password domains

Configure in the Admin / Security panel.

×

⚠ Make sure OpenSSL (Tiki18+) / Mcrypt (Tiki pre-18) is available




Before you enable "User Encryption", make sure that the OpenSSL (Tiki18+) / Mcrypt (Tiki pre-18) PHP extension is available. It is required to encrypt the passwords securely.

User Encryption   

Enable personal, secure storage of sensitive data, e.g. passwords

Requires the mcrypt PHP extension for cryptation. [Check Now](#)
. You may also want to add the "Domain Password" module somewhere.

Comma separated list of password domains, e.g.: Company ABC,Company XYZ
The user can add passwords for a registered password domain.

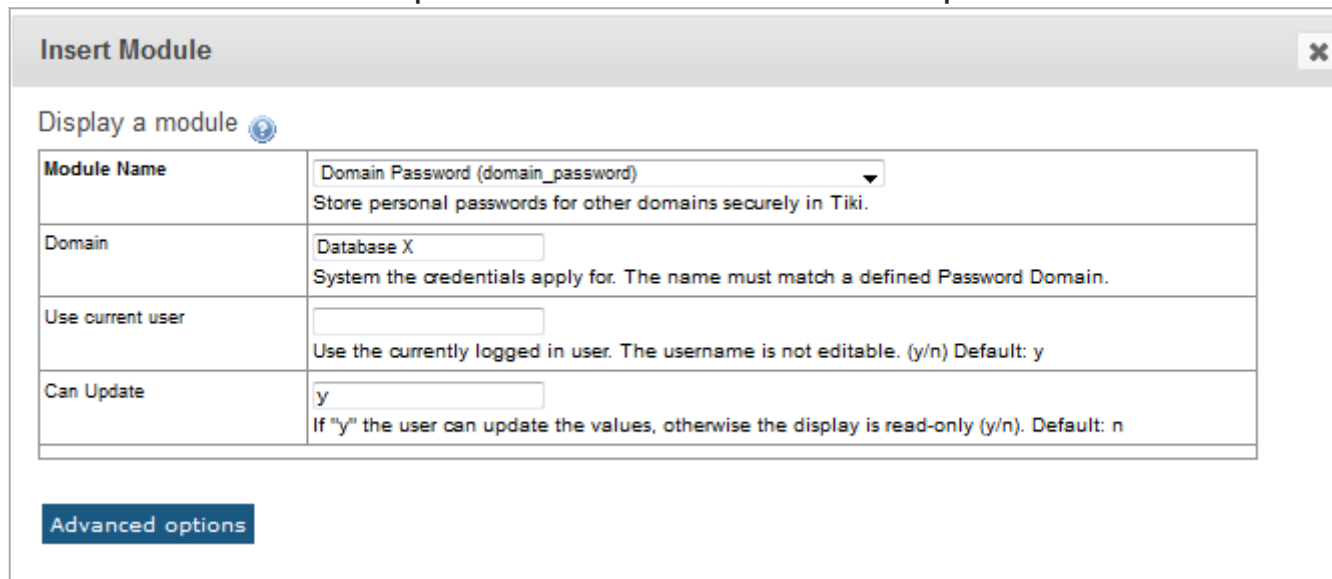
Password Domains:   

Click to expand

The names of the password domains must be unique.

Specifying domain credentials

The module "Domain Password" allows users to specify a password (and possibly a username) for a domain. Only defined password domains can be specified.



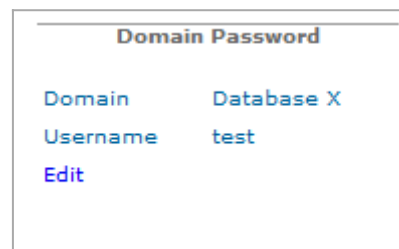
The screenshot shows a dialog box titled "Insert Module" with a close button (X) in the top right corner. Below the title bar, there is a section "Display a module" with a help icon. The main content is a table with four rows:

Module Name	Domain Password (domain_password) [dropdown] Store personal passwords for other domains securely in Tiki.
Domain	Database X [input] System the credentials apply for. The name must match a defined Password Domain.
Use current user	[input] Use the currently logged in user. The username is not editable. (y/n) Default: y
Can Update	y [input] If "y" the user can update the values, otherwise the display is read-only (y/n). Default: n

At the bottom left of the dialog, there is a blue button labeled "Advanced options".

By default the currently logged in Tiki username will be used. By setting "Use current user" = "n", the user must also specify a username.

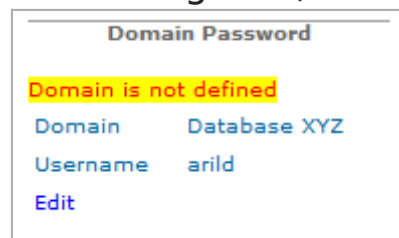
The view mode is displayed initially. The user can choose to edit the credentials, if the module configuration allows it.



The screenshot shows a box titled "Domain Password" containing the following text:

Domain Database X
Username test
Edit

If the password domain is misconfigured, an error message is displayed.

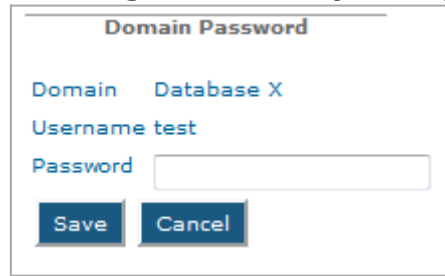


The screenshot shows a box titled "Domain Password" containing the following text:

Domain is not defined
Domain Database XYZ
Username arild
Edit

If the user click edit, the credentials can be edited.

If the current Tiki user is being used, only the password can be edited.



Domain Password

Domain Database X

Username test

Password

Save Cancel

Code integration

See User Encryption @ dev.tiki.org