Shamir's Shared Secrets and Team Password Management via Trackers

This feature introduced in Tiki22 allows you to encrypt password or any other sensitive info with an encryption key. These passwords or sensitive data are stored in the Trackers based on Shamir's Shared Secret algorithm. This is an improved version of shared secret encryption (symmetrical encryption) as we do not need to secure shared keys to the point where they cannot be used alone to decrypt data. Even if a hacker accesses the Tiki database, he still won't be able to decrypt the data (easily) without a second shared key. None of the users will be able to decrypt the data alone without the key in the Tiki database. We use https://github.com/teqneers/shamir

Overview

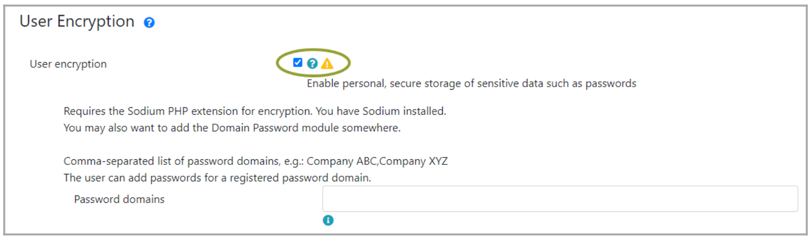
Imagine a door lock that requires at least 3 keys at the same time to open it. So, if you divide the secret key into 5 parts and give them to different users and use a minimum threshold of 3, at least 3 people must provide their share in order to reconstruct the secret. What will happen ? Here is the idea:

- encrypt password or any other sensitive info with an encryption key
- run the key through SSS algorithm with number of shares = number of people to be shared with + 1 and threshold of 2
- store one of the shares in Tiki db
- distribute the rest of the shares to all people that need access to the sensitive info
- then, whenever someone comes, they supply their shared secret and we use the other one stored in Tiki db. Since threshold is 2, they will be able to decrypt the sensitive info.
- This goes beyond the User Encryption feature.

How it works ?

Requirement

Starting with the activation of User encryption that requires the Sodium PHP extension for encryption otherwise, you will not be able to activate it. **"*Settings*" > "*Security*" > "*Control Panels*" > *Search box and search for* "*user encryption*" *preference*** (And once it is active, it can be found at: https://example.org/tiki-admin.php?page=security#content_admin1-1).



User Encryption

User encryption ☑

Enable personal, secure storage of sensitive data such as passwords

Requires the Sodium PHP extension for encryption. You have Sodium installed.
You may also want to add the Domain Password module somewhere.

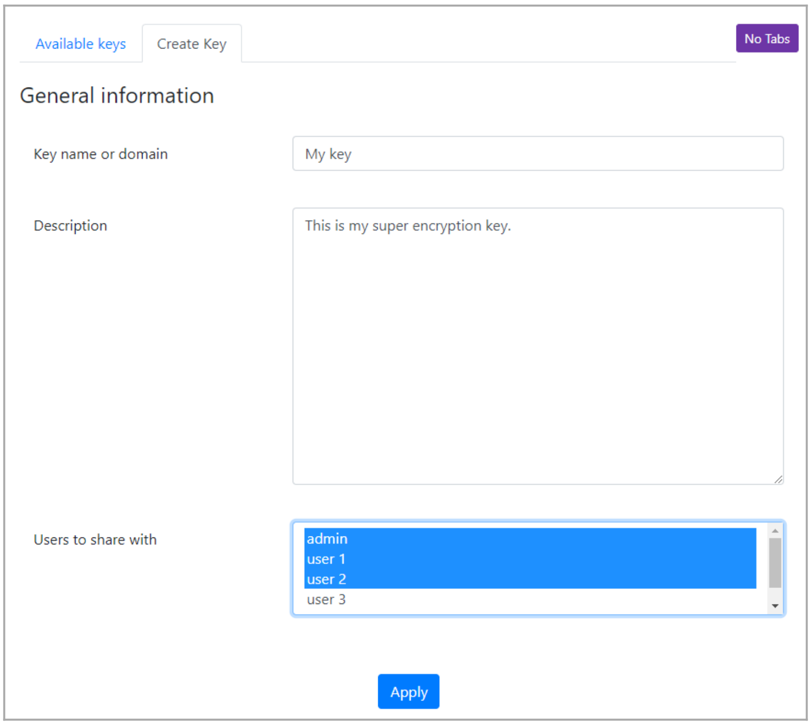
Comma-separated list of password domains, e.g.: Company ABC,Company XYZ
The user can add passwords for a registered password domain.

Password domains

Click to expand

Create encryption key

Once "User encryption" is active, you can then proceed to create the key by proceeding as follows: **"*Settings*" > "*Control Panels*" > "*Security*" > "*Encryption*" *tab* > "*Create key*" *tab*** (https://example.org/tiki-admin.php?page=security#contentencryption-2)



General information

Key name or domain: My key

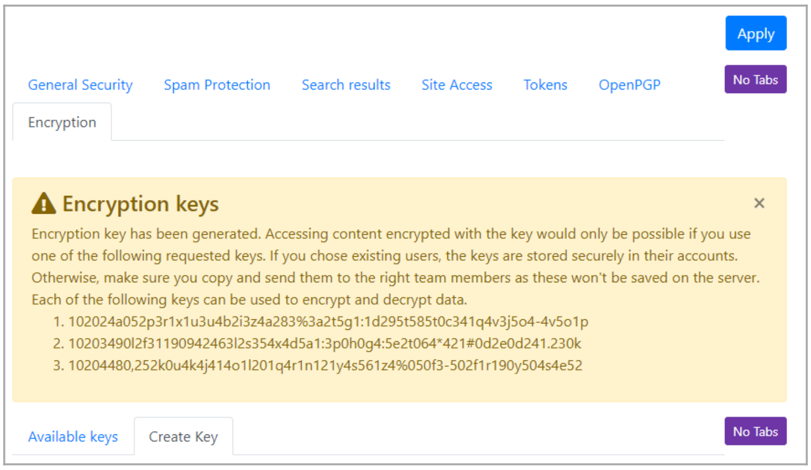
Description: This is my super encryption key.

Users to share with: admin, user 1, user 2 (selected); user 3

Click to expand

Generated keys

After the creation of the encryption key, a number of keys will be generated according to the number of selected users, each of which can be used to encrypt and decrypt data.



⚠ Encryption keys

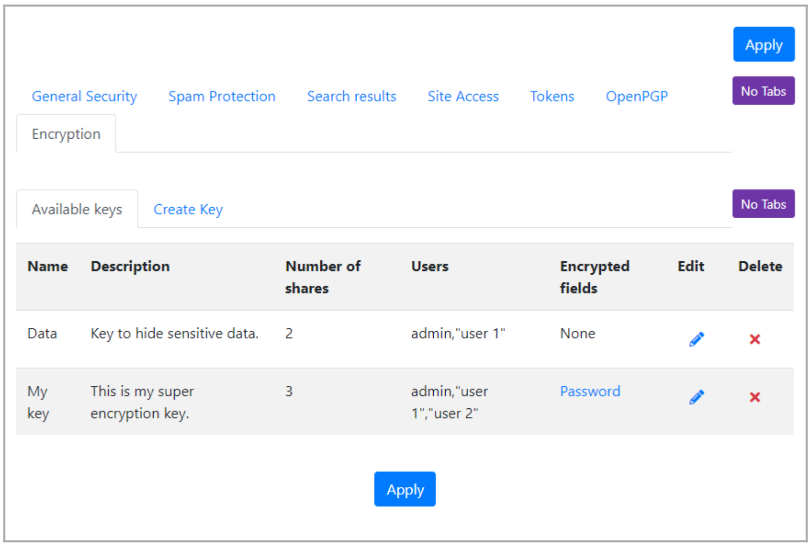
Encryption key has been generated. Accessing content encrypted with the key would only be possible if you use one of the following requested keys. If you chose existing users, the keys are stored securely in their accounts. Otherwise, make sure you copy and send them to the right team members as these won't be saved on the server. Each of the following keys can be used to encrypt and decrypt data.

1. 102024a052p3r1x1u3u4b2i3z4a283%3a2t5g1:1d295t585t0c341q4v3j5o4-4v5o1p
2. 10203490l2f31190942463l2s354x4d5a1:3p0h0g4:5e2t064*421#0d2e0d241.230k
3. 10204480,252k0u4k4j414o1l201q4r1n121y4s561z4%050f3-502f1r190y504s4e52

Click to expand

Encrypted keys list

When changing encryption key, enabling the option **"*Regenerate shares*"** will create new secret shares with the defined number of shares. Old shares will no longer be valid, so you will need to distribute the new shares to team members again. Data encrypted with existing key will stay intact and new shares will be able to decrypt it.
No data loss occurs as long as you keep the shared keys known. Use this option to increase or decrease the number of people with shared keys for this domain. If User Encryption is turned on, newly generated keys will be automatically saved to relevant user accounts.
You add the name of the key, the description and you select the users to share it with.
All the encryption keys added are listed: (https://example.org/tiki-admin.php?page=security#contentencryption-1)

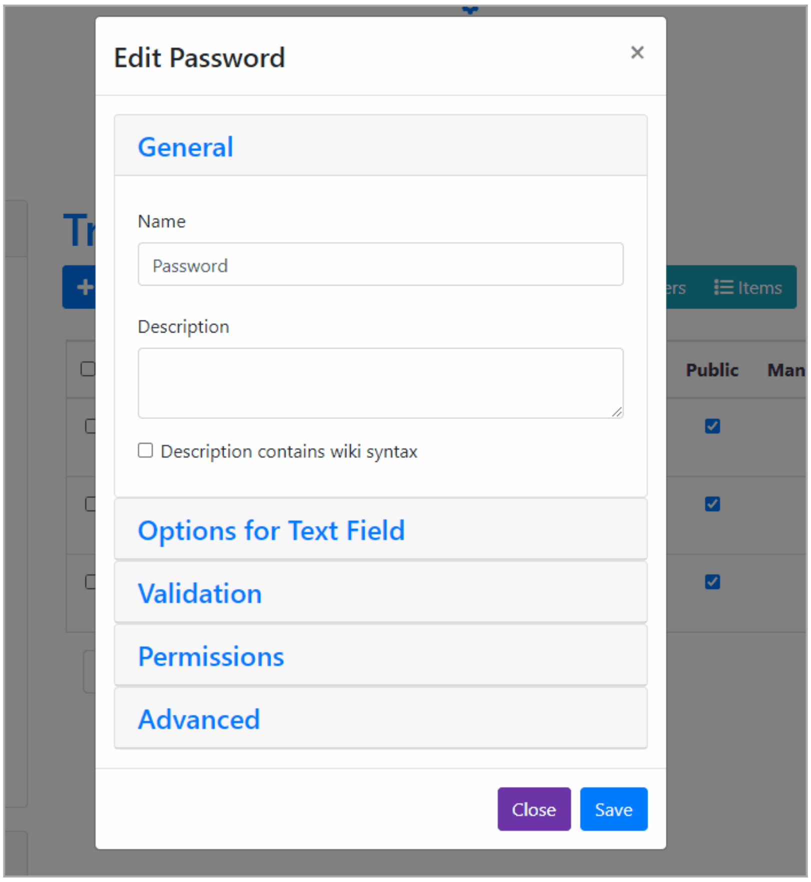


Name	Description	Number of shares	Users	Encrypted fields	Edit	Delete
Data	Key to hide sensitive data.	2	admin,"user 1"	None	✎	✕
My key	This is my super encryption key.	3	admin,"user 1","user 2"	Password	✎	✕

Click to expand

Add encryption option to field

It is, therefore, necessary to create a Tracker to take advantage of the benefits of this feature.
You have to change the "Encryption key" parameter of the field you want to create. This parameter is found in **"*Advanced Options*" *> in the tab* "*Advanced*" *> the field* "*Encryption key*"*, select the key***.



Name: Password

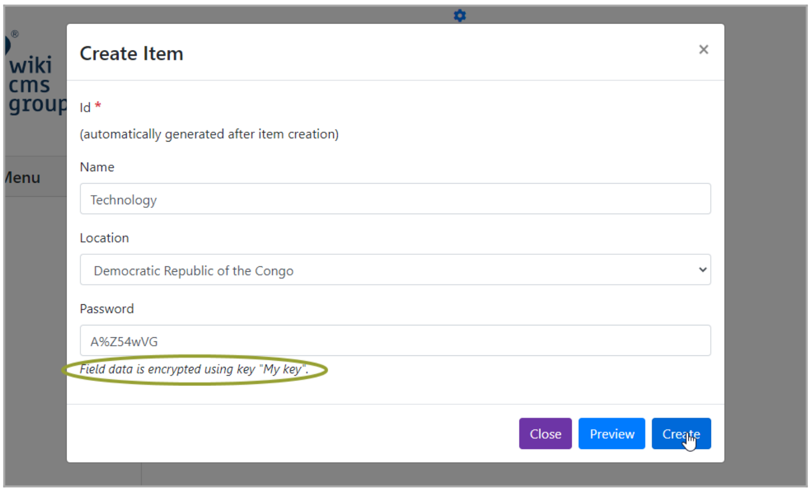
Description:

□ Description contains wiki syntax

Click to expand

Create Tracker item

When creating the item, you will see the message "Field data is encrypted using key" followed by the name of the key used below the field. As on the image below:



Create Item

Id *

(automatically generated after item creation)

Name: Technology

Location: Democratic Republic of the Congo

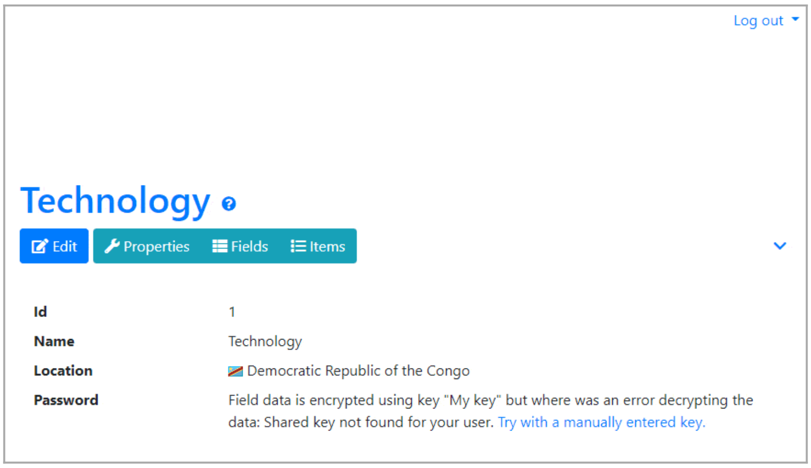
Password: A%Z54wVG

Field data is encrypted using key "My key".

Click to expand

Using keys

We copied one of the keys to finally use it and have access to the encrypted information.



Technology

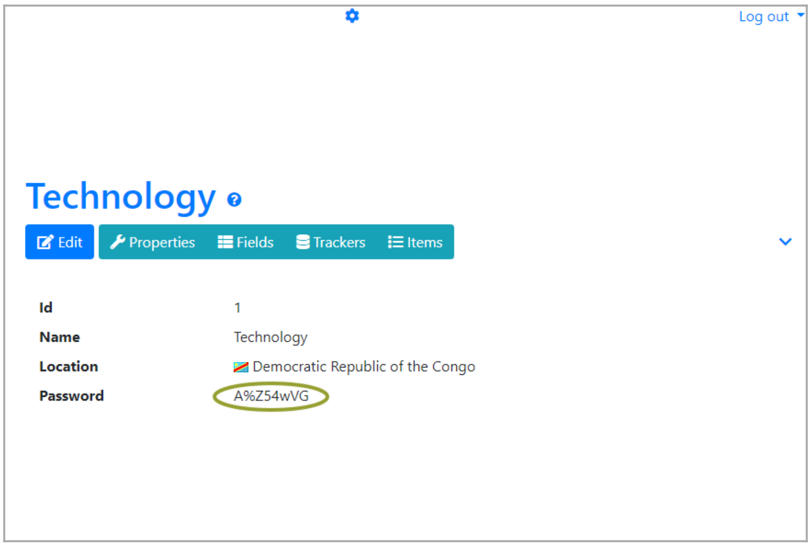
Id	1
Name	Technology
Location	Democratic Republic of the Congo
Password	Field data is encrypted using key "My key" but where was an error decrypting the data: Shared key not found for your user. Try with a manually entered key.

Click to expand

If when using a key you see the message "***Given keys are incompatible***", this is a case where you are using a different key from those generated by the key, it is the same case when you see the message "***Given keys vary in key length***".

Notes

- Users with whom the keys have been shared have direct access to the data of the encrypted fields regardless of the group they belong to as in this case with the user "admin", i.e. they do not need to use their key to decrypt the item field. Remember that the key was initially shared with two other users: "user 1" and "user 2" during its creation.

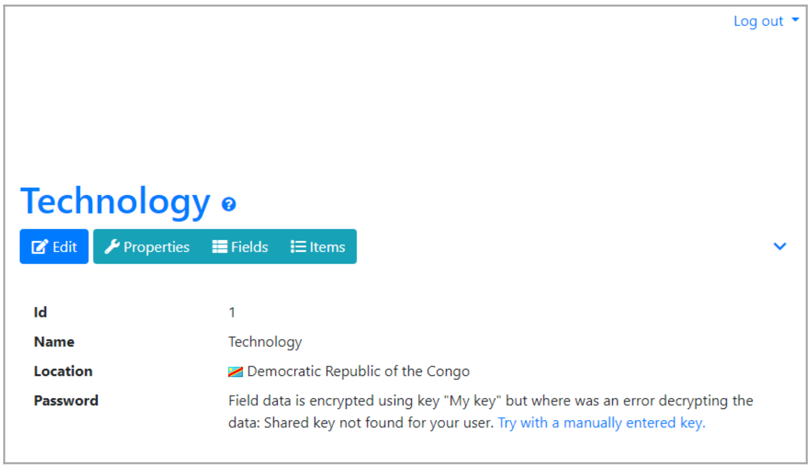


Technology

Id	1
Name	Technology
Location	Democratic Republic of the Congo
Password	A%Z54wVG

Click to expand

- Tracker permissions must be changed to allow non-admin users to access it.
- Other users with whom the key has not been shared must use the key to access the field data because it is hidden from them.



Id	1
Name	Technology
Location	Democratic Republic of the Congo
Password	Field data is encrypted using key "My key" but where was an error decrypting the data: Shared key not found for your user. Try with a manually entered key.

Click to expand

Related

- Old PayPal story: https://www.youtube.com/watch?v=MzescXc5SW0