PluginTOTP

What is Time-Based One-Time Password?

A time-based one-time password **(TOTP)** is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors. Time-based one-time passwords are commonly used for Two-factor authentication and have seen growing adoption by cloud application providers. TOTPs are derived from a secret seed password given at user registration in the form of QR code or in plaintext. TOTPs (and their seeds) are deployed on either hardware security tokens or as soft tokens, meaning mobile device apps that display the numbers. Typically, the temporary passcode expires after 30, 60, 120 or 240 seconds.

TOTP (Time-based One-time Password algorithm) is a different use case than Two-factor authentication, which protects a Tiki instance. This permits to manage the key (instead of putting on a smartphone) to connect to another site (which may or many not be a Tiki)

Using PluginTOTP in Tiki!

Let's suppose I am trying to connect to my Admin Dashboard, I begin by entering my username and password. Then I'm prompted for the TOTP, which I read off of the token and type into the third login field. Once I've done so, I'm logged.

Parameters

Allows to generate Time-based One-time Password

Go to the source code
Preferences required: wikiplugin_totp

Parameters	Accepted Values	Description	Default	Since
`interval`		Amount of seconds that a TOTP will be valid/refreshed		
`issuer`		Name of the application where the generated time-based one-time password will be used.		
`secret`		Secret key required to generate time-based one-time passwords. If not provided, a new secret key will be generated automatically.		

Step 1 : Activate pluginTOTP

Go to Control Panel, search TOTP, check the PluginTOTP preferences and Click Apply to save changes.
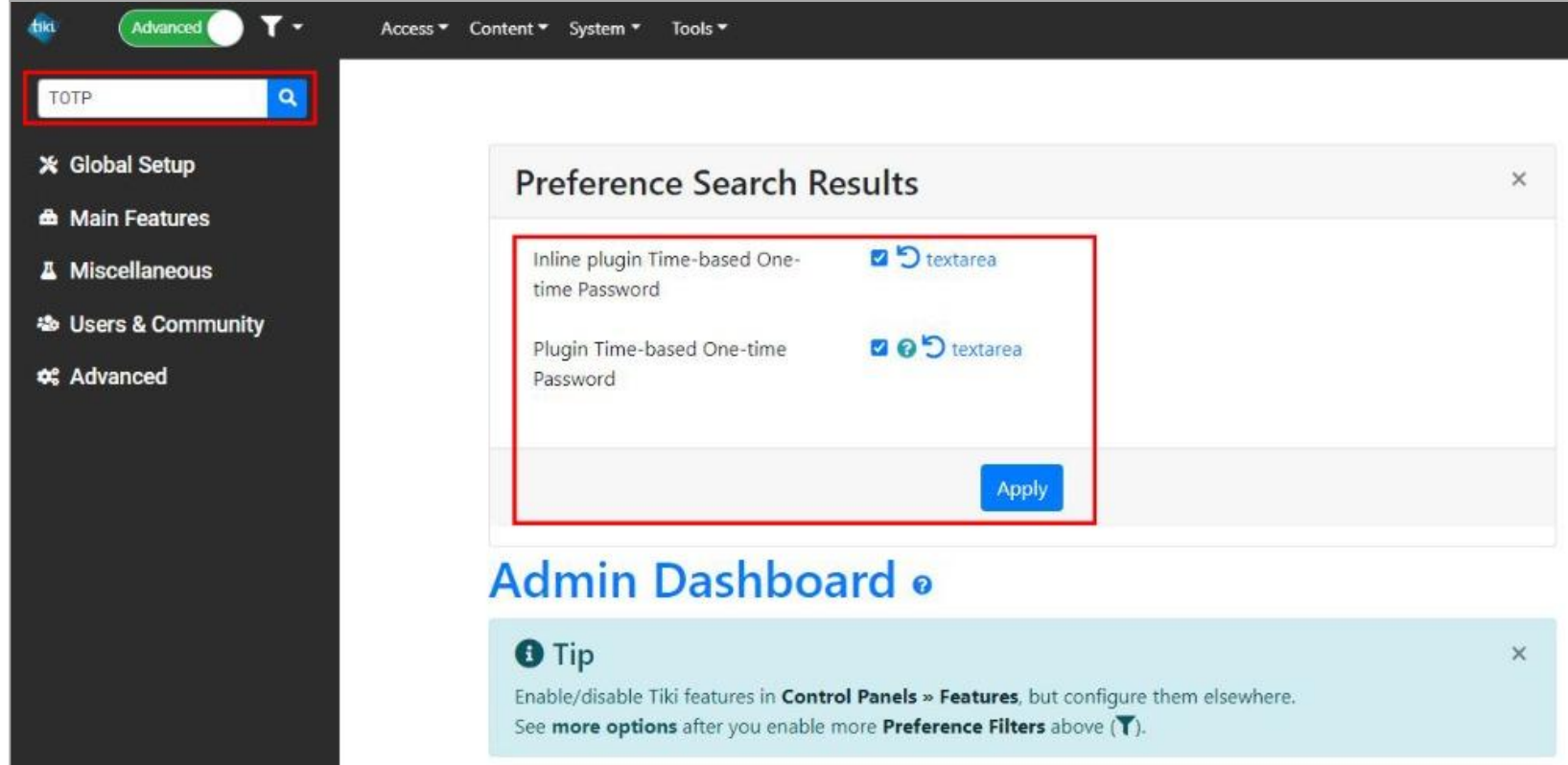
Click to expand

Step 2 : Configure pluginTOTP

You need to setup a wiki login page with following input fields :

・Username Field

・Password Field

・TOTP Code Field

✕

ⓘ Tip

{totp secret="YOUR SECRET TOTP CODE" interval="INTERVAL IN SECONDS" issuer="YOUR ISSUER PAGE"}
The secret key must be 16 characters long and contain only uppercase letters A-Z and digits 2-7, otherwise it

will not generate the Qr code. If you don't know the secret you can live it blank and Tiki will generate a secret for you.

If you want to use advanced options of the pluginTOTP, click at the ⊙Help button (at right corner of your wiki-page editor), search TOTP in PluginHelp tab.''

You should now see something like this

Code: **114702** Expires in: 12 seconds.

Hide QRCode

1. Install Google Authenticator® app on your device and open it.
2. Tap "Scan a barcode".
3. Scan the QR code that is open in your browser.
4. Done, Google Authenticator® is now generating codes.

Click to expand

Step 3 : Authenticate

Finally, when authenticating on page "Log In" (e.g. http://www.example.com/tiki-login_scr.php?totpForm), take the code generated by your TOTP app (Google Authenticator® App or other) and enter it in the **totpCode Field you recently created** then Click to Login.

You need to act fast because these codes start expiring, which if you're too slow, sometimes yields a login misfire

and you need to try again with a fresher TOTP.

See also :
Two-factor authentication