

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. TOTP is derived from a secret seed password given at user registration in the form of QR code or in plaintext. TOTP (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

[Go to the source code](#)

Preferences required: wikipugin_totp

Parameters	Accepted Values
<code>interval</code>	
<code>issuer</code>	
<code>secret</code>	

Description

Amount of seconds that a TOTP will be valid/refreshed

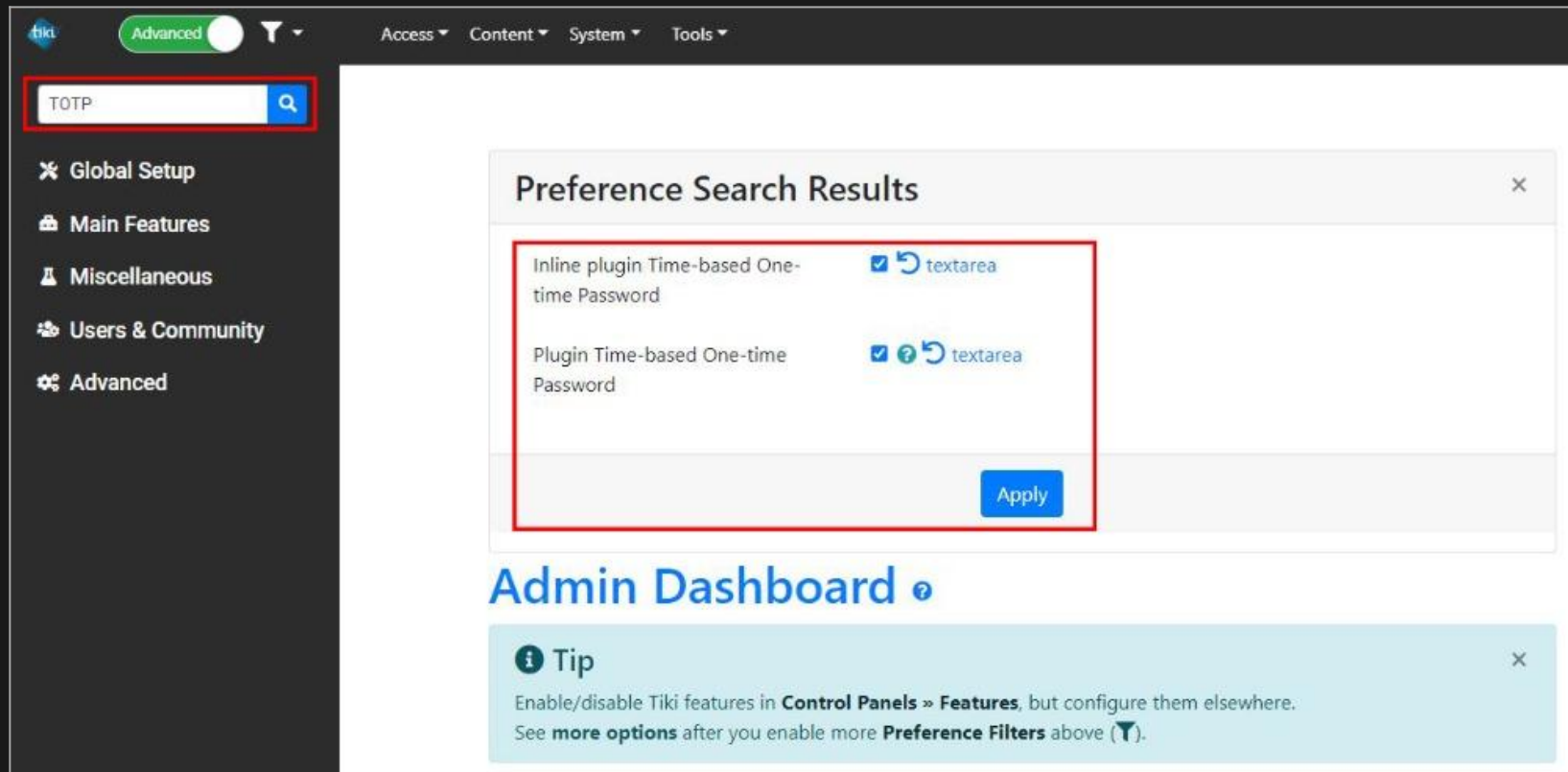
Name of the application where the generated time-based one-time password will be use.

Secret key required to generate time-based one-time passwords

Default	Since

STEP 1 : ACTIVATE PLUGINTOTP

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



The screenshot shows the Tiki Admin Dashboard interface. On the left, a search bar contains the text 'TOTP'. Below it, a sidebar lists navigation options: Global Setup, Main Features, Miscellaneous, Users & Community, and Advanced. The main content area displays 'Preference Search Results' for 'TOTP'. Two preference items are listed, both with checked boxes and 'textarea' labels: 'Inline plugin Time-based One-time Password' and 'Plugin Time-based One-time Password'. An 'Apply' button is located at the bottom right of the search results box. Below the search results, there is an 'Admin Dashboard' section with a 'Tip' message: 'Enable/disable Tiki features in Control Panels » Features, but configure them elsewhere. See more options after you enable more Preference Filters above (T).'

Click to expand


STEP 2 : CONFIGURE PLUGINTOTP

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






```
{totp secret="YOUR SECRET TOTP CODE" interval="INTERVAL IN SECONDS" issuer="YOUR ISSUER PAGE"}
```

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:  Expires in: -- 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](#)