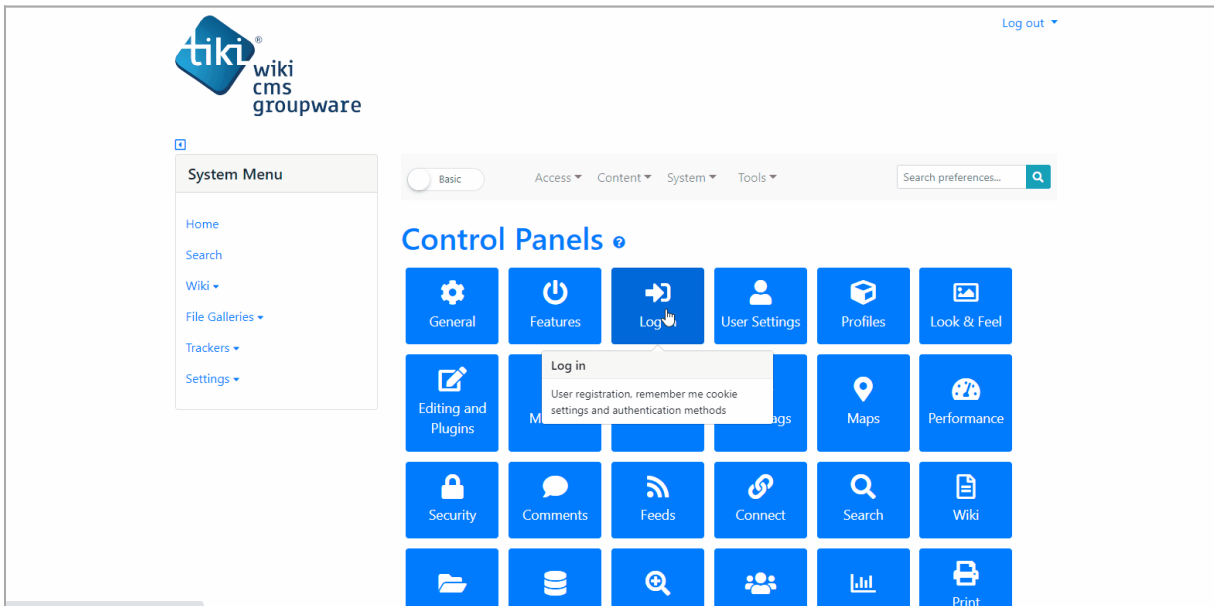


# Steps

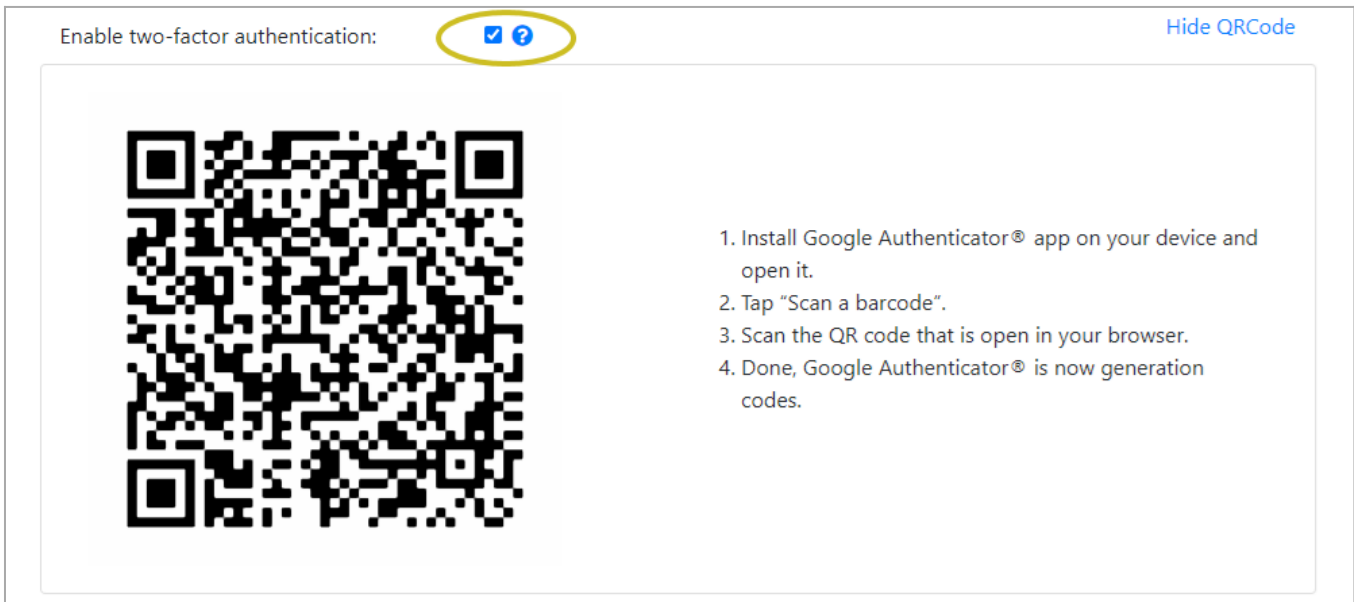
**Step 1:** First enable the "Allow users to use 2FA" option in the "Log In" feature in your Tiki, go to **Settings** → **Control Panels** → **Log In** → **General Preferences** tab "tiki-admin.php?page=login#contentadmin\_login-1" (e.g [http://www.example.com/tiki-admin.php?page=login#contentadmin\\_login-1](http://www.example.com/tiki-admin.php?page=login#contentadmin_login-1)) with "Preference Filters" to Advanced.



Click to expand

**Step 2:** Next, install Google Authenticator® App on your mobile phone. [See how to install it here.](#)

**Step 3:** Check the "Enable two-factor authentication" option in the "User Preferences" page, the "Account Information" tab and click on "Save changes" button. Note that the current password is required to make changes. At this step, you need to connect Tiki and the Google Authenticator® application by scanning the QR Code generated in the "User Preferences" page. Click on "Show QRCode" to display the QR Code, scan it using the application you installed in step 2.



Click to expand

**Step 4:** Finally, when authenticating on page "Log In" (e.g. [http://www.example.com/tiki-login\\_scr.php?twoFactorForm](http://www.example.com/tiki-login_scr.php?twoFactorForm)), take the code generated by Google Authenticator® App and enter it in the field "Two-factor Authenticator Code".

The image shows a 'Log In' form with the following elements:

- Log In** (Section Header)
- Username:** Input field containing the letter 'I'
- Password:** Input field
- [I forgot my password](#) (Link)
- Two-factor Authenticator Code:** Input field
- Log in** (Blue Button)
- [Register](#) (Link)

Click to expand

By adhering to standardized algorithms like TOTP and HOTP, 2FA solutions become both secure and flexible. These methods make user authentication robust and effective.

## Related links

- Original commit: <http://sourceforge.net/p/tikiwiki/code/70793>

## Page aliases

---

- [2FA](#)