

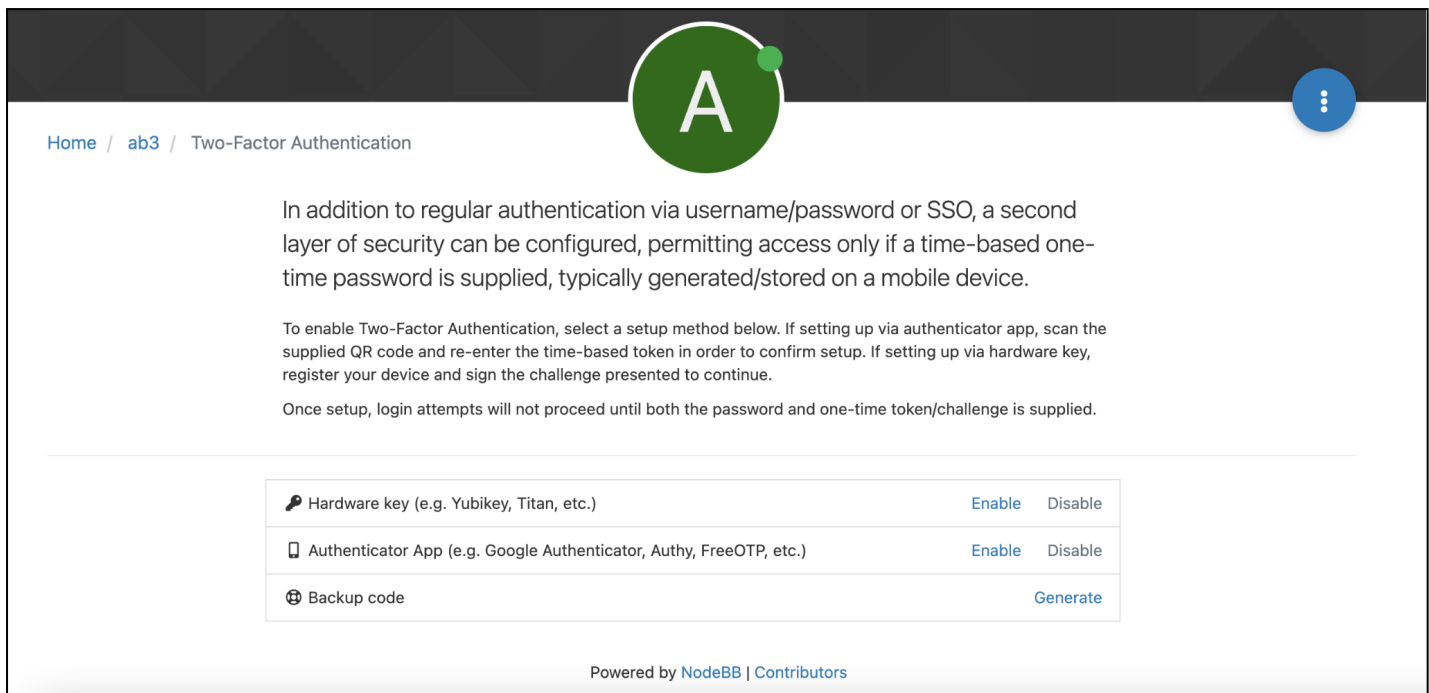


Steps for Configuration as Admin

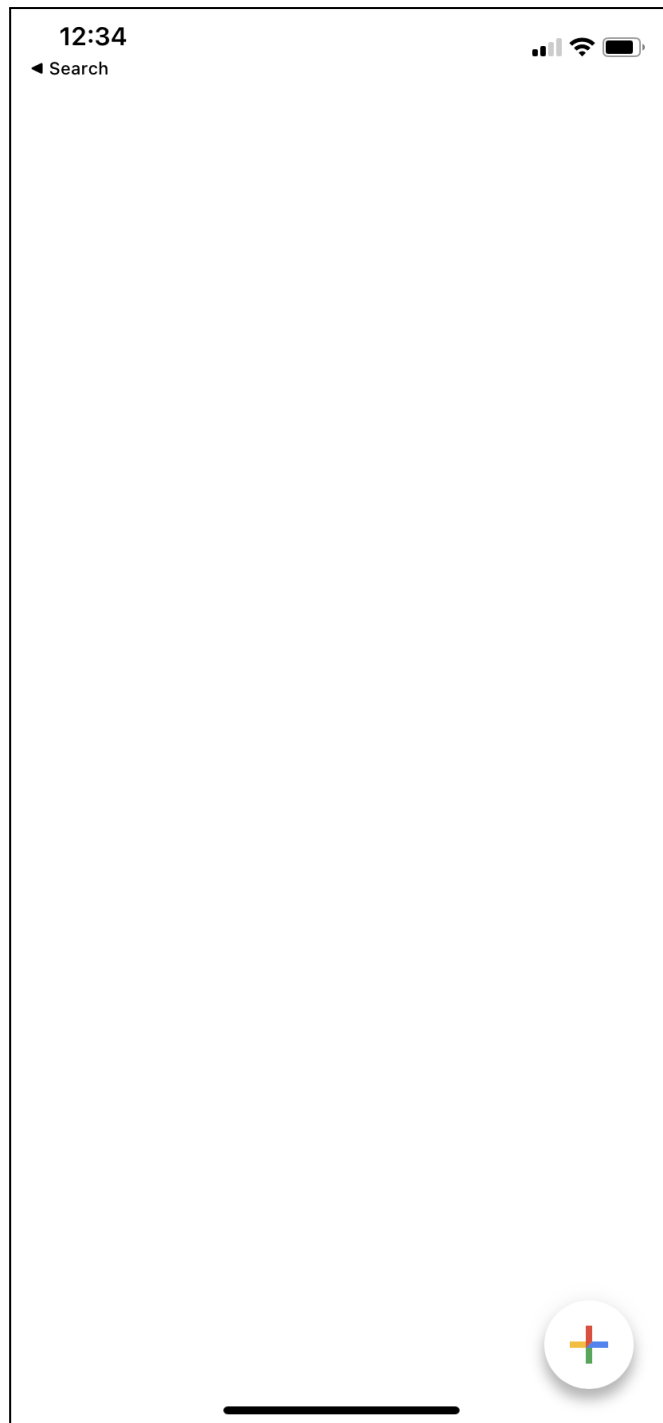
1. Login to the admin account using the respective credentials, to enable two-factor authentication for all users on the application.
2. Select the "Admin" tab on the top of the page.
3. Select "Extend" and select "Plugins" from the dropdown menu.
4. Under the "Plugin Search" bar, enter the following: "nodebb-plugin-2factor". This is what will be used to enable the countermeasure.
5. Select "Activate" which will open up a window where "Confirm" can be selected.
6. On the top of the page, click on on this following button to restart and rebuild the page to enable to installed plugin: .
7. Select Plugins, and select "Two-Factor Authentication" from the dropdown menu.
8. Under the "Enforce 2Factor Authentication", select all the administrators and users, and click on the blue save icon: .
9. Now, Two-Factor Authentication should be enabled for all accounts and future accounts under the application.

Steps for Configuration as User (using Google Authenticator)

1. (Return back to these steps after completing a creation of an account if not already made)
2. Login to your account with the respective username and password
3. The following page will be displayed:



4. Under Authenticator App, select “Enable”, which should display a QR code and token.
5. Go to your mobile device and install the “Google Authenticator” application
6. Open up the application and the following should be displayed:



7. Select the Plus Icon at the bottom right of the screen.
8. Select “Scan a QR code” which will use the QR code provided from the NodeBB application.
9. Scan the QR code with your camera.
10. Now the code will be associated and displayed on your Google Authenticator Screen.
11. Enter the code into the text box to confirm the association, and select “Confirm”.

The QR code shown above will allow you to associate your mobile device (via the GAuthenticator app or a suitable variant) with your account on this website. Simply scan it via the app, and key in the generated token to confirm.

12. Enter the code displayed on the Google Authenticator application once again into the input box:

Two-Factor Authentication

Enter the verification code generated by your mobile application.

Verify

[← Back to choices](#)

13. Now, two-factor authentication is enabled with your account.

Steps to Login with Two-Factor Authentication

1. Enter your Username and Password on the Login page.
2. Enter the six-digit code displayed on the Google Authenticator application in the following box and select “Verify”:

Two-Factor Authentication

Enter the verification code generated by your mobile application.

Verify

[← Back to choices](#)

- Now, you are successfully authenticated and logged in to the account