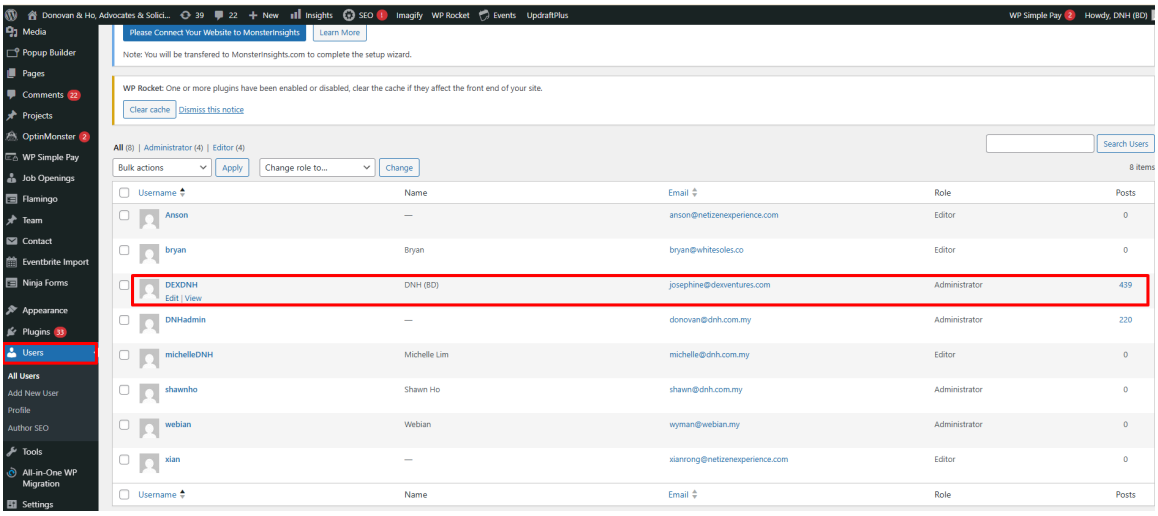
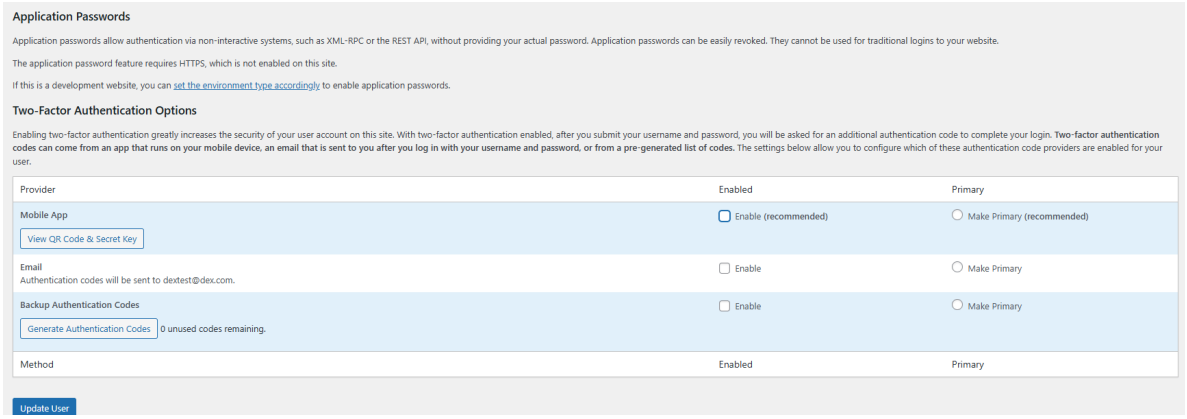
How to setup 2FA using Solid Security

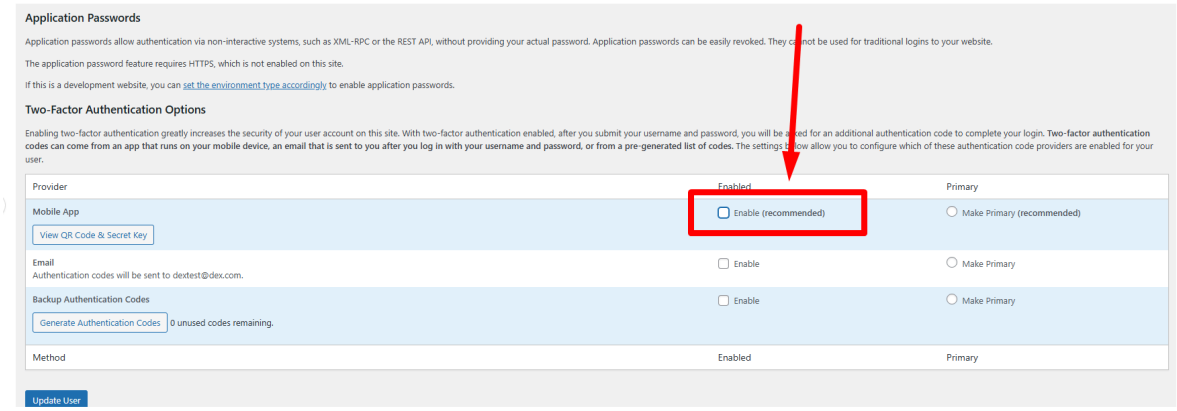
1. The user who wants to enable 2FA should first log in to their account in the backend.
2. Then click on “Users” from the left menu and edit their profile.



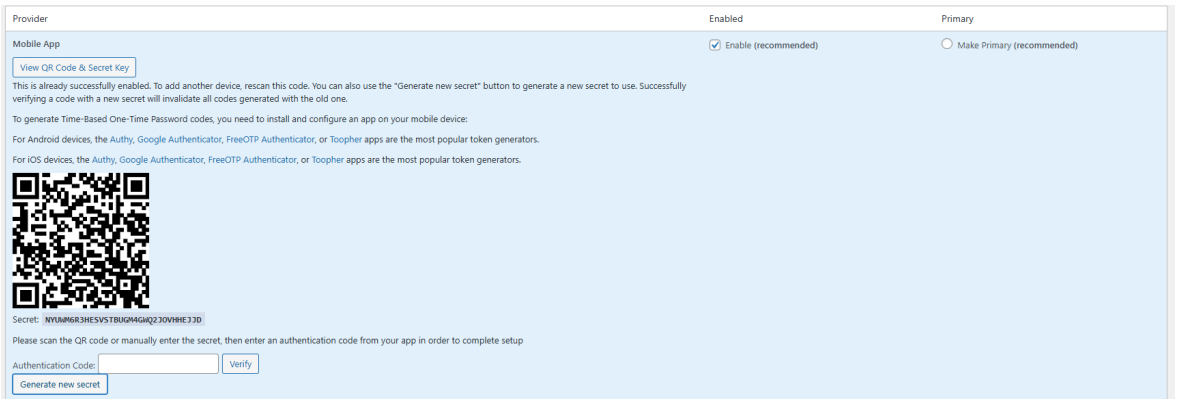
3. Scroll down to the bottom of the Edit Profile page, where you will find the option to set up 2FA.



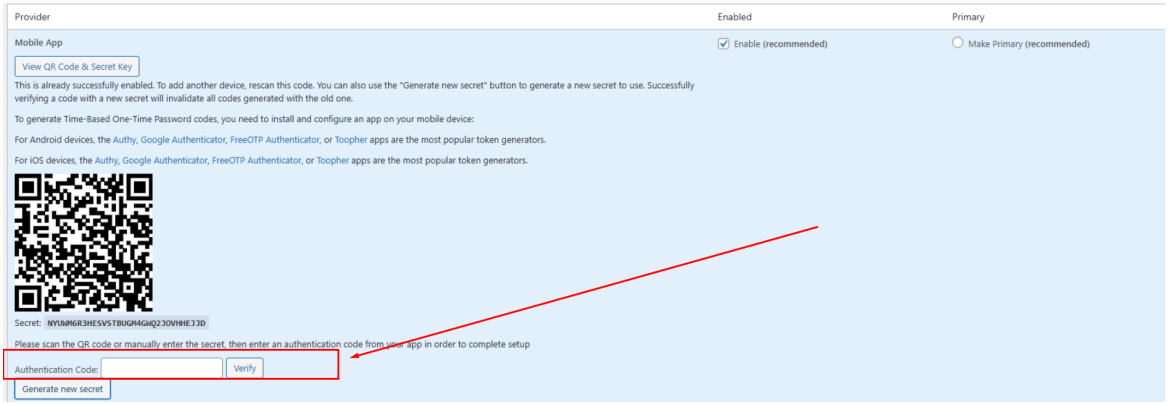
4. There will be three options: Mobile App, Email, and Backup Authentication.
5. If you want to set it up through a mobile app, you need to download an authenticator app on your phone. We recommend using the Google Authenticator app.
6. Then enable the Mobile App option.



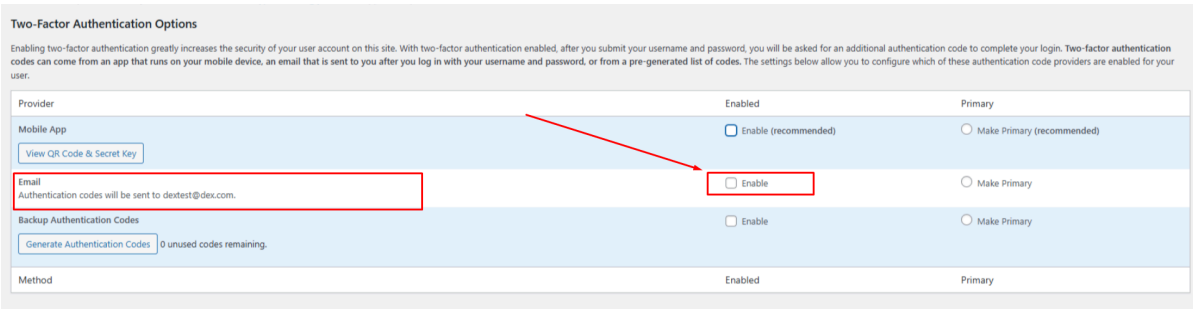
7. You will see a QR code displayed. Scan this QR code using the Google Authenticator app installed on your phone.



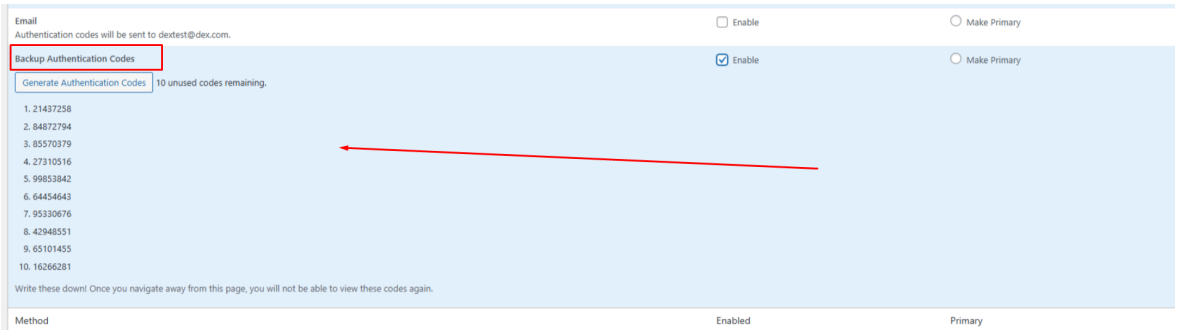
8. The app will show a time-based code that keeps changing. Enter that code into the authentication code field on the website and verify it.



9. If you want to set it up through email, enable the Email option. A code will be sent to your email, which you need to enter on the website in the authentication code field and verify.



10. The last option is Backup Authentication. You will receive a set of backup codes — save them securely. These codes can be used if you ever lose access to your Google Authenticator app or email.



11. And then, whenever you log in next time, after entering your credentials, it will ask for 2FA. You will need to enter the latest code from the Google Authenticator app at the time of login.

Note: And if it doesn't work the first time, then go back to the user details again. At the bottom, you will see the option to "Configure." Click on Configure, and the same setup options will appear in a popup. This time you just need to complete it once, you don't need to enter all the details again like the previous steps. Simply follow the steps by clicking Next and then Done.

Thanks