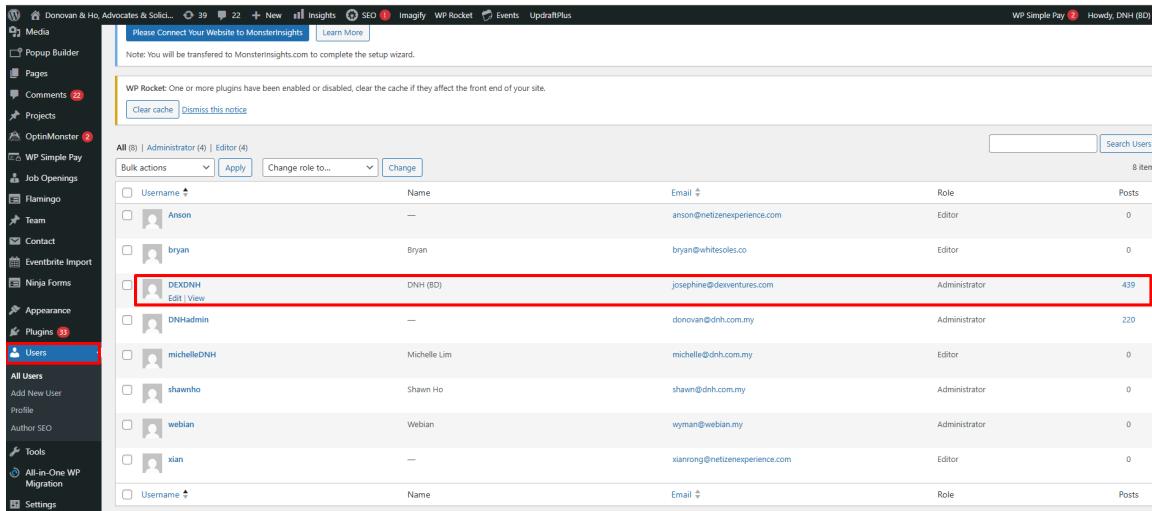


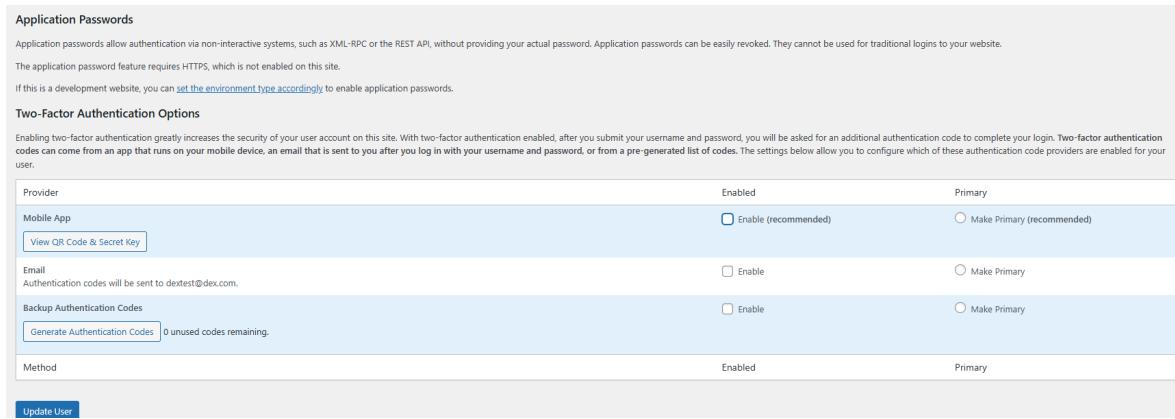
# How to setup 2FA using Solid Security

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.



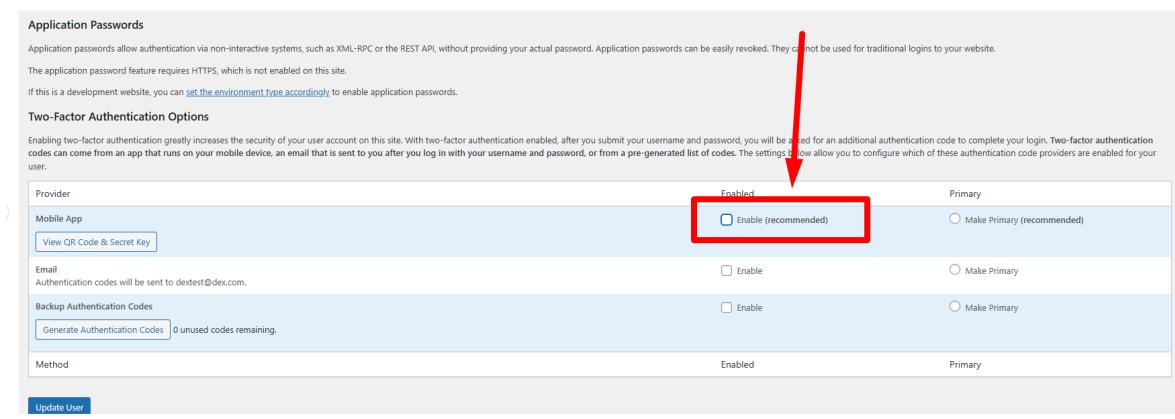
The screenshot shows the WordPress admin dashboard under the 'Users' section. A list of users is displayed, including 'Anson', 'bryan', 'DEXDNH', 'DNHadmin', 'michelleDNH', 'shawhho', 'webian', and 'xian'. The user 'DEXDNH' is highlighted with a red box. The 'DEXDNH' row contains the name 'DNH (BD)', email 'josephine@cleverventures.com', role 'Administrator', and posts '439'. There are also 'Edit' and 'View' buttons for this user.

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



The screenshot shows the 'Edit Profile' page for the user 'DEXDNH'. In the 'Two-Factor Authentication Options' section, the 'Mobile App' provider is selected. The 'Enable (recommended)' checkbox is checked, and the 'Make Primary (recommended)' radio button is selected. Other providers like 'Email' and 'Backup Authentication Codes' are also listed with their respective enablement options.

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.



The screenshot shows the 'Edit Profile' page for the user 'DEXDNH'. In the 'Two-Factor Authentication Options' section, the 'Mobile App' provider is selected. The 'Enable (recommended)' checkbox is checked, and the 'Make Primary (recommended)' radio button is selected. Other providers like 'Email' and 'Backup Authentication Codes' are also listed with their respective enablement options. A red arrow points to the 'Enable (recommended)' checkbox.

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

Provider	Enabled	Primary
Mobile App	<input checked="" type="checkbox"/> Enable (recommended)	<input type="radio"/> Make Primary (recommended)
<a href="#">View QR Code &amp; Secret Key</a> <p>This is already successfully enabled. To add another device, rescan this code. You can also use the "Generate new secret" button to generate a new secret to use. Successfully verifying a code with a new secret will invalidate all codes generated with the old one.</p> <p>To generate Time-Based One-Time Password codes, you need to install and configure an app on your mobile device:</p> <p>For Android devices, the Authy, Google Authenticator, FreeOTP Authenticator, or Toopher apps are the most popular token generators.</p> <p>For iOS devices, the Authy, Google Authenticator, FreeOTP Authenticator, or Toopher apps are the most popular token generators.</p>  <p>Secret: NVUNGRHESVSTBUHMGH0230VHEJJD</p> <p>Please scan the QR code or manually enter the secret, then enter an authentication code from your app in order to complete setup</p> <p>Authentication Code: <input type="text"/> <a href="#">Verify</a></p> <p><a href="#">Generate new secret</a></p>		

- 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.

Provider	Enabled	Primary
Mobile App	<input checked="" type="checkbox"/> Enable (recommended)	<input type="radio"/> Make Primary (recommended)
<a href="#">View QR Code &amp; Secret Key</a> <p>This is already successfully enabled. To add another device, rescan this code. You can also use the "Generate new secret" button to generate a new secret to use. Successfully verifying a code with a new secret will invalidate all codes generated with the old one.</p> <p>To generate Time-Based One-Time Password codes, you need to install and configure an app on your mobile device:</p> <p>For Android devices, the Authy, Google Authenticator, FreeOTP Authenticator, or Toopher apps are the most popular token generators.</p> <p>For iOS devices, the Authy, Google Authenticator, FreeOTP Authenticator, or Toopher apps are the most popular token generators.</p>  <p>Secret: NVUNGRHESVSTBUHMGH0230VHEJJD</p> <p>Please scan the QR code or manually enter the secret, then enter an authentication code from your app in order to complete setup</p> <p>Authentication Code: <input type="text"/> <a href="#">Verify</a></p> <p><a href="#">Generate new secret</a></p>		

- 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.

Two-Factor Authentication Options		
<p>Enabling two-factor authentication greatly increases the security of your user account on this site. With two-factor authentication enabled, after you submit your username and password, you will be asked for an additional authentication code to complete your login. Two-factor authentication codes can come from an app that runs on your mobile device, an email that is sent to you after you log in with your username and password, or from a pre-generated list of codes. The settings below allow you to configure which of these authentication code providers are enabled for your user.</p>		
Provider	Enabled	Primary
Mobile App	<input checked="" type="checkbox"/> Enable (recommended)	<input type="radio"/> Make Primary (recommended)
Email Authentication codes will be sent to dextest@dex.com.	<input type="checkbox"/> Enable	<input type="radio"/> Make Primary
Backup Authentication Codes	<input type="checkbox"/> Enable	<input type="radio"/> Make Primary
<a href="#">Generate Authentication Codes</a> 0 unused codes remaining.		
Method	Enabled	Primary

- 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.

Two-Factor Authentication Options		
<p>Enabling two-factor authentication greatly increases the security of your user account on this site. With two-factor authentication enabled, after you submit your username and password, you will be asked for an additional authentication code to complete your login. Two-factor authentication codes can come from an app that runs on your mobile device, an email that is sent to you after you log in with your username and password, or from a pre-generated list of codes. The settings below allow you to configure which of these authentication code providers are enabled for your user.</p>		
Provider	Enabled	Primary
Mobile App	<input checked="" type="checkbox"/> Enable (recommended)	<input type="radio"/> Make Primary (recommended)
Email Authentication codes will be sent to dextest@dex.com.	<input type="checkbox"/> Enable	<input type="radio"/> Make Primary
<a href="#">Generate Authentication Codes</a> 10 unused codes remaining.		
<p>1. 21472728 2. 84872794 3. 85570379 4. 27310516 5. 99853842 6. 64454643 7. 95330676 8. 42948551 9. 65101455 10. 16266281</p> <p>Write these down! Once you navigate away from this page, you will not be able to view these codes again.</p>		
Method	Enabled	Primary

- 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