Time-Based One-Time Passwords (TOTP)

Download the PDF of this article.

In this Article

Related Articles

Overview

Time-Based One-Time Passwords, or TOTP, are a common method to provide secondary authentication to online accounts. Using an app on your phone like Google Authenticator, Authy, etc., you can generate a "one-time password" that changes after a period of time, usually thirty seconds. TOTP ensures that only those with access to your phone (to get the code from the authenticator app) can authenticate into your account. Also, even if a malicious individual can get one of your codes through other means, they have a short expiration time.

Who can use TOTP authentication in FormAssembly?

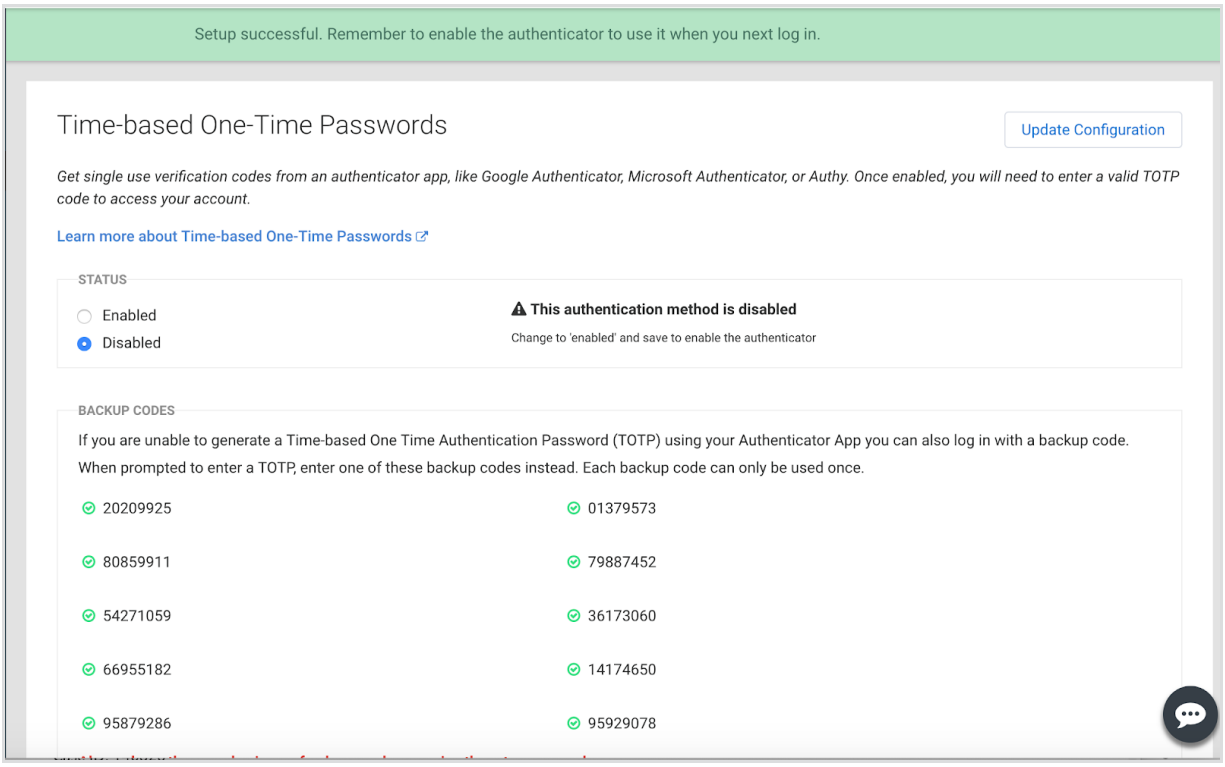
TOTP authentication is available to our Essentials plan and higher customers.

What do I need?

You will need a mobile phone or other mobile device and an authenticator app like Google Authenticator, Authy, LastPass Authenticator, Microsoft Authenticator, etc.

How do I set up my TOTP authenticator on FormAssembly?

- To start, add TOTP to your multi-factor authenticator timeline. For instructions on adding an MFA method to your timeline, reference the Multi-factor Authentication article.
- In the multi-factor authenticator timeline screen, click **Configure** for your TOTP authenticator.
- For a first-time setup, you will immediately be taken to the setup screen with a QR code to scan. Use your authenticator app's QR code scanning function to do this.
    - Hover the viewfinder over the QR code on the screen and it will automatically register the TOTP account on your device.
    - If you cannot use the QR scanning function, the secret key is displayed below the QR image for manual entry in your authenticator app.
- Once the account has been registered on your authenticator app, it will generate a new six-digit code every thirty seconds. To verify correct registration and complete the setup process, enter a valid six-digit code within the time window and submit the verification.
- Upon success, you will see a message indicating the setup was successful.



The TOTP authenticator is now set up to use, you will need your TOTP authenticator the next time you log in to your FormAssembly account.

How do I log in with my TOTP authenticator?

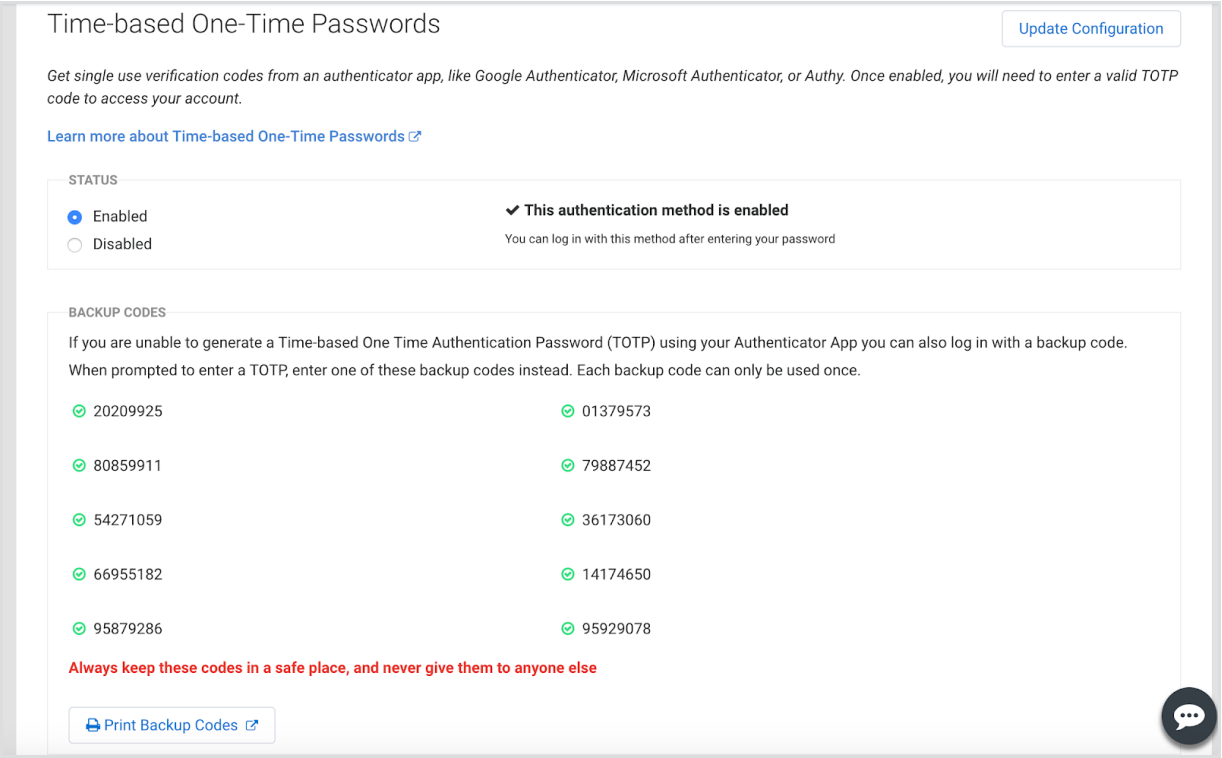
- Enter your credentials on the login page.
- You will be taken to the TOTP authenticator challenge. Enter the current six-digit code on your device for FormAssembly into the text box and submit it. Be sure to do this before the current code expires and a new one is generated.
- If successful, you will be taken into your account.

What are my backup codes?

Your backup codes are a collection of ten eight-digit codes that can each be used once instead of a TOTP code generated by your device. They are there so that you may still get into your account using TOTP authentication if you do not have access to your device for whatever reason. Each code is single-use, and will visually indicate when it is used. We recommend printing these codes and keeping them in a secure location. Note that you should treat these backup codes with the same care that you would treat your device that generates your TOTP codes, as they can allow access to your account by attackers if compromised.

How do I print out my backup codes?

- After you have set up your TOTP authenticator, navigate to the main landing page for your TOTP authenticator. There you will see your backup codes.



- Click **Print Backup Codes**, for a print-friendly page containing your current backup codes.
- The page will automatically prompt you to print the codes. You may also use your browser's native print functionality to do so.

How do I generate new backup codes?

- Navigate to your **Multi-factor Authenticators** page under your user profile settings.
    - Hover over your username
    - Click Account
    - Click **Configure MFA**
- **Delete** your current TOTP authenticator.
- Re-add TOTP by clicking **Configure** and scanning the new QR code with your authenticator app (Google Authenticator, Authy, etc.).
- Once set up, a fresh set of 10 backup codes will be generated and displayed on the TOTP authenticator page.
