

Two-Factor Authentication or 2FA

Hamid Semiyari

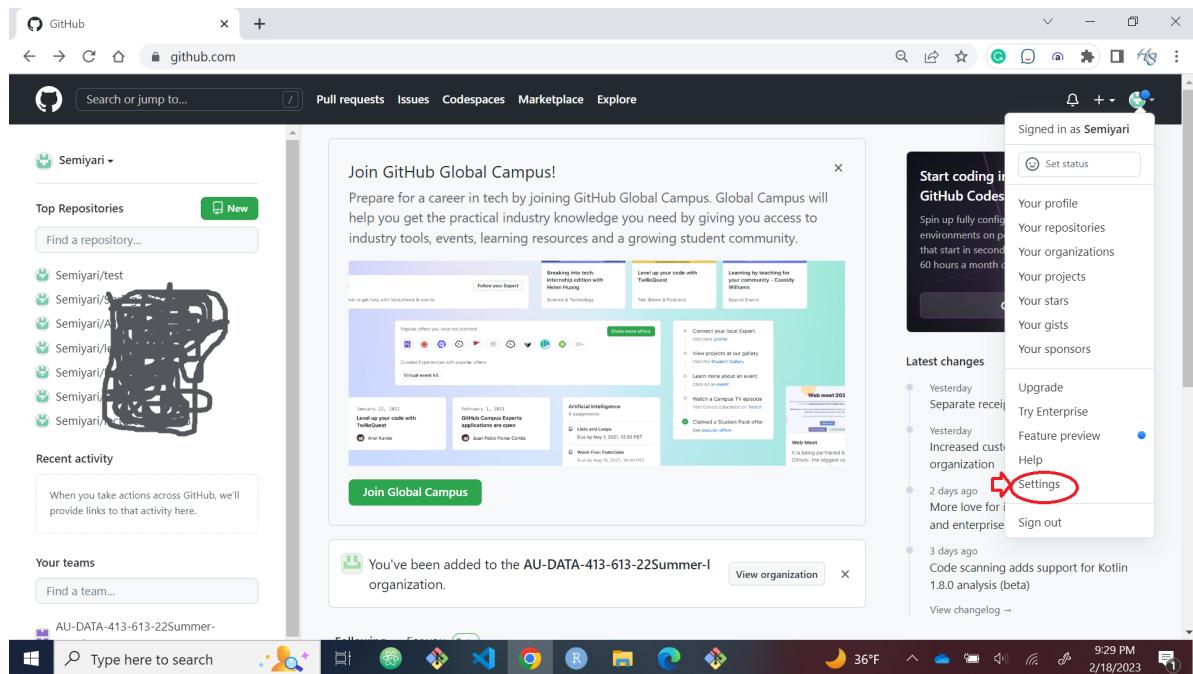
A quick or summary Note about authentication with GitHub

- Prior to August 13, 2021, you were allowed to authentication by typing username and password before you can access certain resources on GitHub. For instance every time you pushed or pulled from GitHub. Using your GitHub password is no longer allowed.

You can access your resources in GitHub in a variety of ways: in the browser, via GitHub Desktop or another desktop application, with the API, or via the command line. Each way of accessing GitHub supports different modes of authentication.

Authenticating in your browser

- *Username and password with two-factor authentication or 2FA*
 - You'll create a password when you create your account on GitHub. We recommend that you use a password manager to generate a random and unique password.
 - If you have not enabled 2FA, GitHub will ask for additional verification when you first sign in from an unrecognized device, such as a new browser profile, a browser where the cookies have been deleted, or a new computer. After providing your username and password, you will be asked to provide a verification code that we will send to you via email. If you have the GitHub Mobile application installed, you'll receive a notification there instead.
- Step 1. In the upper-right corner of any page, click on your avatar (or your profile photo), then click *Settings*.



Step 2. Scroll down and click on “Password and authentication”

Basic Git Commands | Atl... x Your Profile x check to see if you already x Use personal access token x Reviewing and revoking p... x +

github.com/settings/profile

Semiyari Your personal account Switch to another account Go to your personal profile

Public profile

- Account
- Appearance
- Accessibility
- Notifications
- Password and authentication**
- Bio
- Sessions
- SSH and GPG keys
- Organizations
- Moderation

Name

Your name may appear around GitHub where you contribute or are mentioned. You can remove it at any time.

Profile picture

Public email

Select a verified email to display

You have set your email address to private. To toggle email privacy, go to [email settings](#) and uncheck "Keep my email address private."

Bio

Tell us a little bit about yourself

URL

https://github.com/settings/security

Step 2. Scroll down and click on “Enable two-factor authentication”,

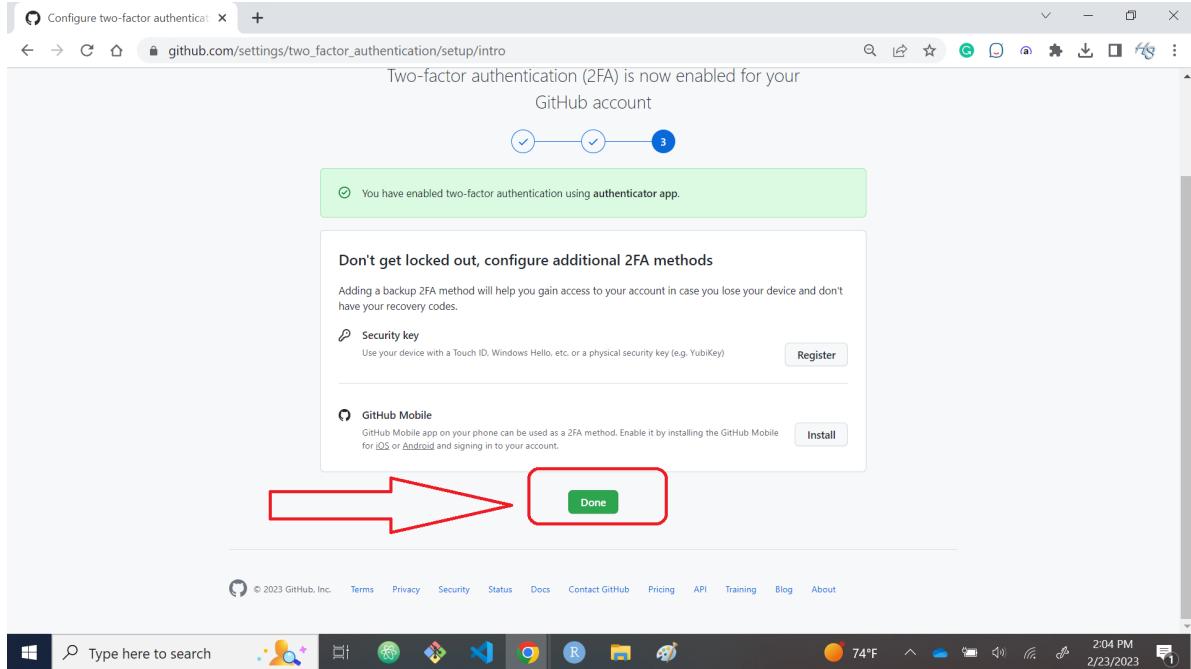
The screenshot shows the GitHub settings interface for two-factor authentication. On the left sidebar, under 'Password and authentication', the 'Sessions' option is selected. The main content area displays a message: 'Two factor authentication is not enabled yet.' It explains that two-factor authentication adds an extra layer of security. Below this is a green button labeled 'Enable two-factor authentication'. A red box highlights this button. At the bottom right of the message area is a link 'Learn more'.

- Step 3. There are a three steps process to follow I used [Duo app](#), which I already had it installed in my phone.

The screenshot shows the 'Enable two-factor authentication (2FA)' setup page. It is step 1 of 3. The first step is 'Setup authenticator app'. It instructs users to use a phone app like Duo, Authy, LastPass Authenticator, or Microsoft Authenticator to get 2FA codes. It provides a QR code for scanning and a text input field for entering the code if scanning fails. A red box highlights the text 'I used the DUO app that I already have for my AU's account'. A green box highlights the text 'Then follow all steps, at the end you will get a code. Type it here'.

- Step 4. You were askto save your recovery code in some safe place.

- Step 5. Last step, they have two options to choose, if you want to.



Authenticating with GitHub Desktop

- You can authenticate with GitHub Desktop using your browser. For more information, see [Authenticating to GitHub](#).

Authenticating with the API

- Personal access token
 - In limited situations, such as testing, you can use a personal access token to access the API. Using a personal access token enables you to revoke access at any time. For more information, see [Creating a personal access token](#).