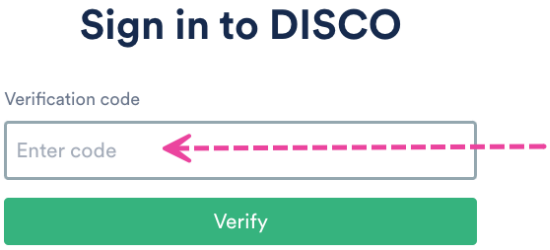
Setting up and using Multi-factor Authentication (MFA)

Last Modified on 06/18/2025 4:58 pm PDT

To help protect your DISCO account, we strongly suggest enabling **Multi-factor authentication (MFA).**

At a glance

Multi-factor authentication (MFA), is an extra security measure that can be enabled on an online account. After entering a username and password to log in, MFA requires users to present one or more additional types of authentication to decrease the chances of the account being compromised. Most commonly, this is in the form of entering a dynamic six-digit verification code.



These verification codes are generated by a third-party authentication app, such as **Google Authenticator**, **Microsoft Authenticator**, and others.

In many cases, passwords alone are not enough to protect online accounts. With MFA enabled, even if a hacker has your password, they won't be able to log into your account unless they have the device with your authenticator app to access the verification codes.

Enabling multi-factor authentication on your DISCO

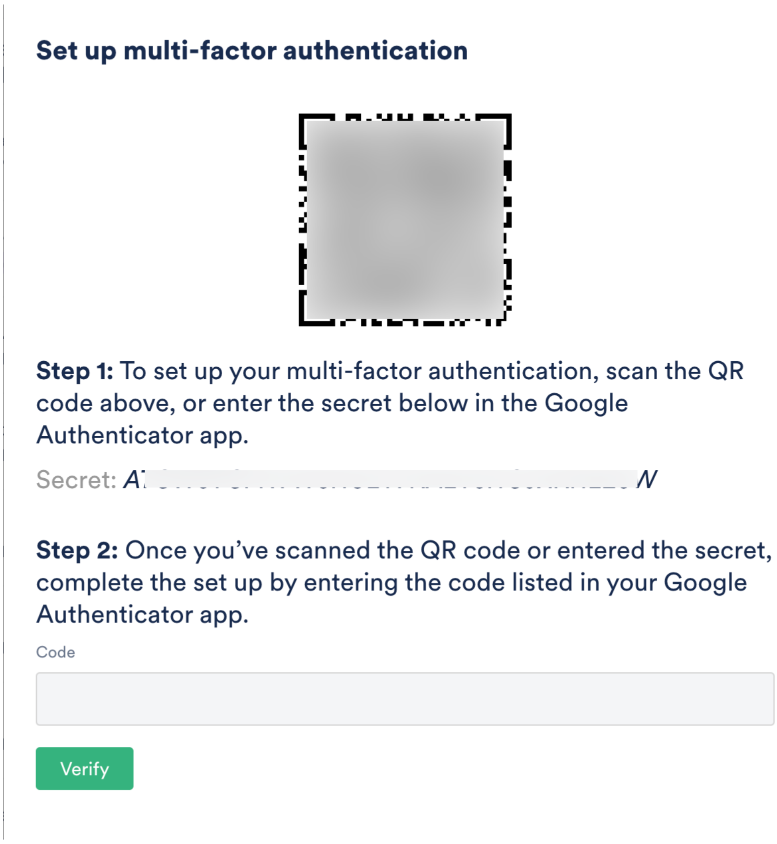
MFA can be enabled on your DISCO by request. Please email support@disco.ac or contact us via chat using the Support menu (question mark) in the bottom-right corner of your DISCO.

> ***Note:*** *When MFA is enabled for one DISCO, if there are users on that DISCO who use the same email address to log in to other DISCOs, they will also be prompted to use MFA when logging in to those other DISCOs.*

Setting up multi-factor authentication

Initial set up prompt

When MFA is first enabled on your DISCO, *all users in your DISCO* will see the following setup prompt the next time they go to log in, just after entering their username and password:



Set up multi-factor authentication

Step 1: To set up your multi-factor authentication, scan the QR code above, or enter the secret below in the Google Authenticator app.

Secret: *A[redacted]N*

Step 2: Once you've scanned the QR code or entered the secret, complete the set up by entering the code listed in your Google Authenticator app.

Code

Notes:

- *The prompt will contain a unique **QR code** and **Secret** for each user. The screenshots in this article are for demonstration purposes only.*
- *Although the prompt mentions **Google Authenticator**, you are not required to use this specific app. You can use any authenticator app you prefer.*

Pre-requisite steps

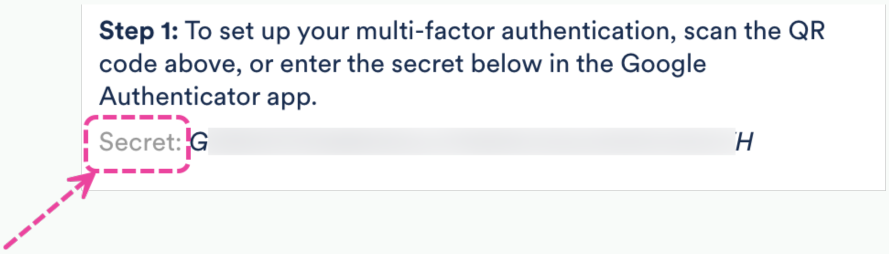
Before beginning the setup process, you will need to:

Choose an authentication device

You can use a mobile device or computer.

Save your Secret from DISCO

Also known as a **Secret Key**, this is the code shown in the MFA setup prompt in DISCO.



Step 1: To set up your multi-factor authentication, scan the QR code above, or enter the secret below in the Google Authenticator app.

Secret: *G[redacted]H*

> ***Important:*** *This code is generated during the setup process and is* ***unique*** *to each user. Keep it in a safe place and* ***do not share*** *it with anyone. It will come in handy if you ever lose your authentication device, as you will need it to set up MFA again on another device.*

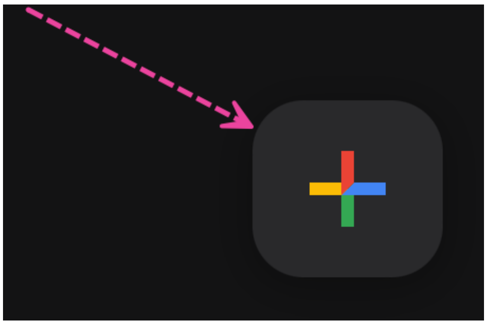
> **□ Install an authentication app or extension**
>
> **□On mobile:**
>
> You can install an authentication app from the Google Play Store (Android) or App Store (iOS). Two well-known authenticator apps are **Google Authenticator** and **Microsoft Authenticator**, but any authenticator app will do.
>
> **□ On your computer:**
>
> You can use a desktop app, or add an extension to your web browser. Some password managers (e.g. **1Password**, etc.) have authentication features built-in for desktop and browser use.

Step 1: Add your DISCO account to your authenticator app

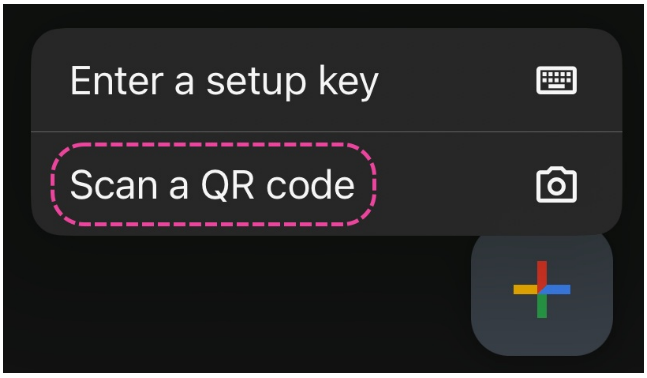
For the sake of simplicity, we have provided instructions below using two well-known authenticator apps: Google Authenticator and Microsoft Authenticator on a mobile device.

Set up MFA using **Google Authenticator** on a **mobile device**:

1. Open the Google Authenticator app on your mobile device.
2. To add a new account, tap the **+ plus** icon on the bottom right.

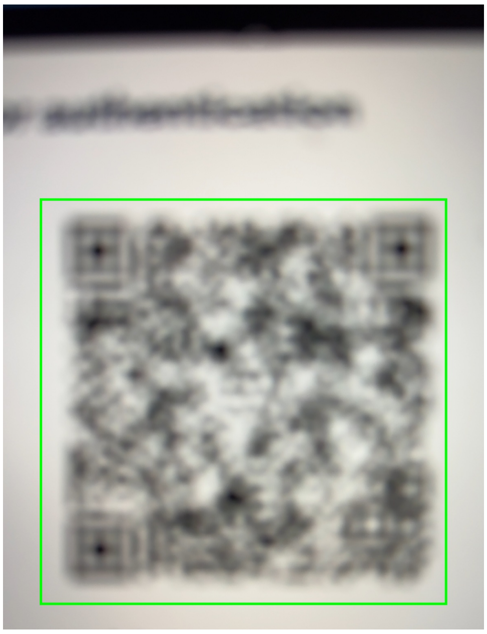


3. Tap **Scan a QR code***. This will open up your camera in barcode scanning mode.

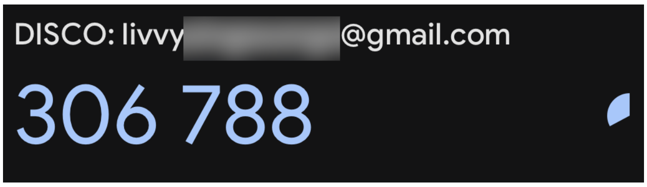


Alternatively, you can tap* ***Enter a setup key**, and enter the* ***Secret*** *key from the prompt in your DISCO.*

4. Hold your mobile device up to your computer screen, with the QR code from the prompt in your DISCO centered in your camera.



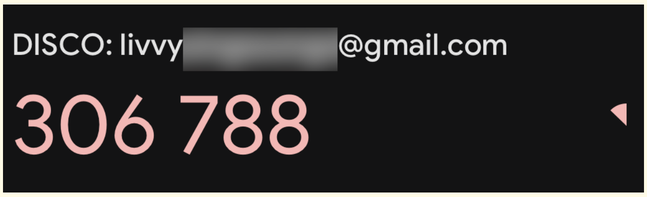
5. A new entry will be created for your DISCO account with a six-digit code underneath it.
6. The code will be valid for 30 seconds until it is replaced by another code, and so on. The timer to the right of the code indicates when the code is about to expire.



DISCO: livvy[redacted]@gmail.com

306 788

Tip: *If the code is red, wait for the next code.*

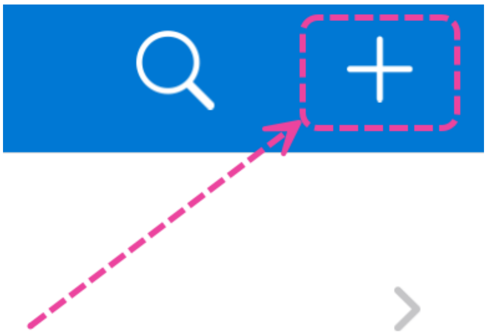


DISCO: livvy[redacted]@gmail.com

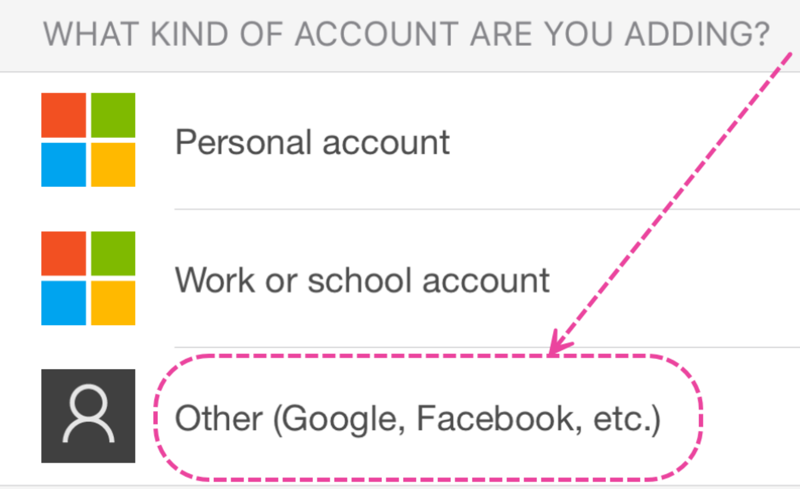
306 788

Set up MFA using **Microsoft Authenticator** on a **mobile device**:

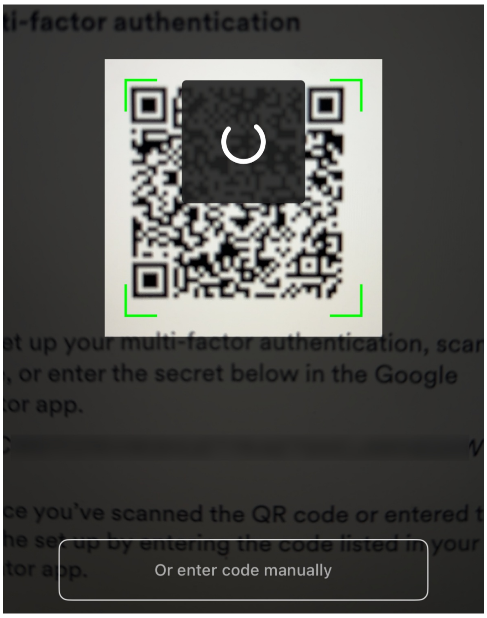
1. Open the Microsoft Authenticator app on your mobile device.
2. To add a new account, tap the **+ plus** icon on the top right.



3. Tap **Other (Google, Facebook, etc.)**.

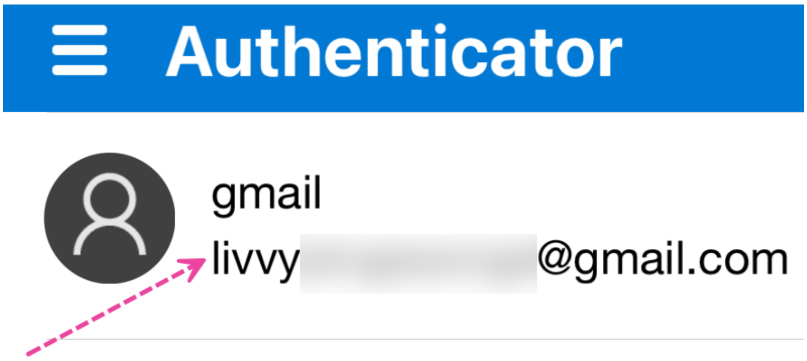

WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
Other (Google, Facebook, etc.)

4. This will open up your camera in barcode scanning mode*.
5. Hold your mobile device up to your computer screen, with the QR code centered in your camera.



Alternatively, you can tap **Or enter code manually, and enter the **Secret** key from the prompt in your DISCO.*

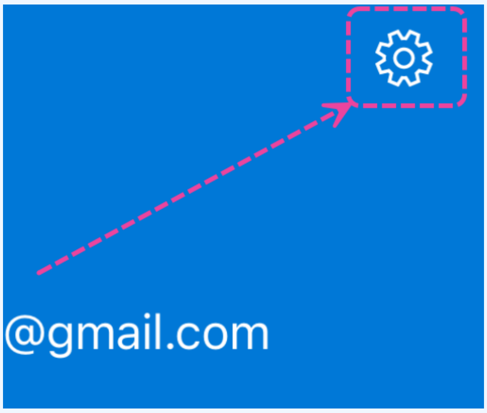
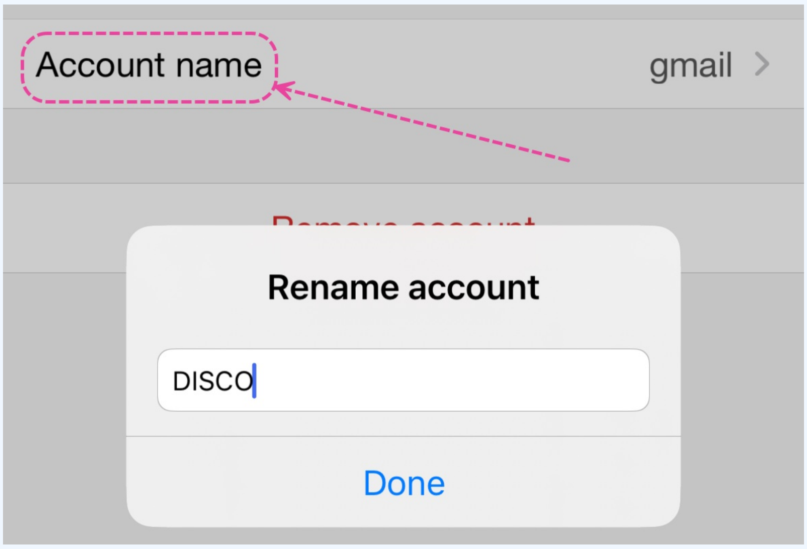
6. A new entry will be created for your DISCO account.



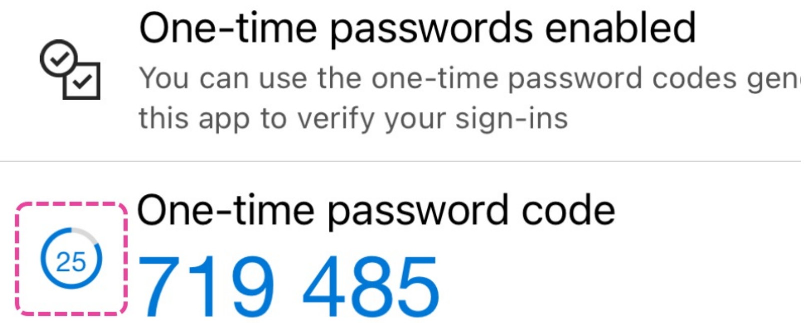
Authenticator

gmail

livvy[redacted]@gmail.com

> ***Note:*** *The entry name will not reference DISCO when created. To rename it, tap on the entry, then tap the gear icon.*
>
> 
>
> @gmail.com
>
> *Tap **Account name**, edit the name, and tap **Done**.*
>
> 
>
> Account name gmail
>
> Remove account
>
> Rename account
>
> DISCO
>
>

7. To access the code, tap on the new account entry.
8. The code will be valid for 30 seconds until it is replaced by another code, and so on. The timer to the left of the code indicates when the code will expire.



One-time passwords enabled

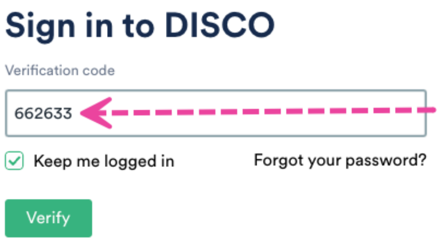
You can use the one-time password codes gen
this app to verify your sign-ins

One-time password code

719 485

Step 2: Enter the six-digit code from your authenticator app into DISCO

Type or paste the code from your authenticator app, and click the **Verify** button.

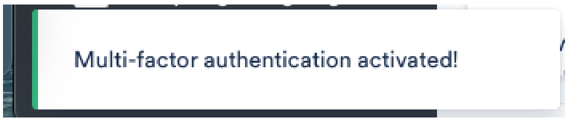


Sign in to DISCO

Verification code: 662633

☑ Keep me logged in

You will then be logged in to your DISCO and a message will appear in the bottom left corner to confirm MFA has been activated:



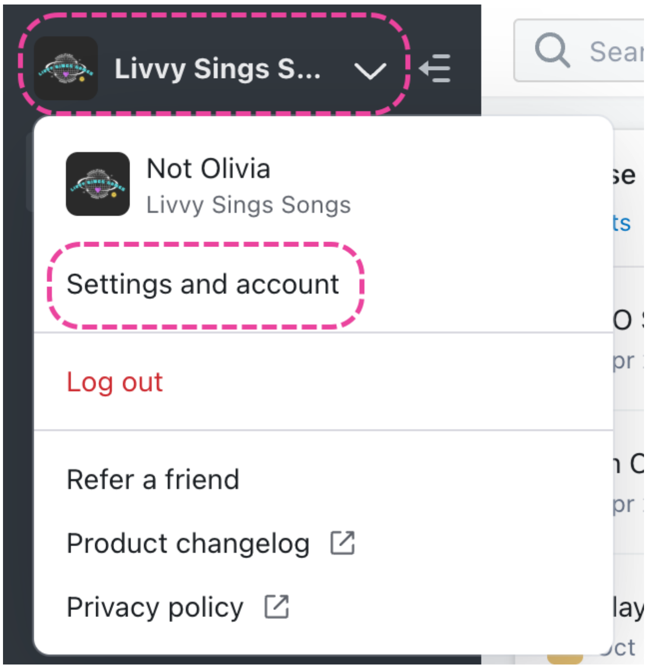
Multi-factor authentication activated!

Resetting multi-factor authentication

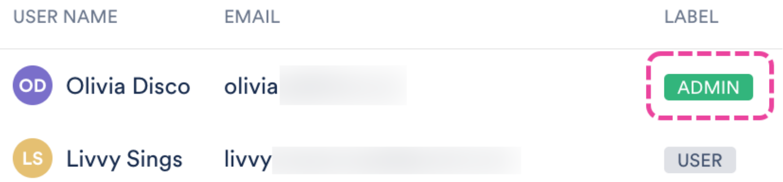
If you no longer have access to the device you set up MFA with or you need to set up a new device, your MFA credentials must be reset. In either case, for security purposes, you will need to send an email to our Support team at support@disco.ac.

We will require verification from one of the Admins on your account, so to expedite matters it's helpful to CC one of your DISCO's Admins on the email. To find out who your account Admins are:

1. In the top-left corner of your DISCO, click on your DISCO Business Name to open the menu.
2. Select **Settings and Account**.



3. Under **Workspace Settings**, select **Users**.
4. Admins will have the **Admin** label to the right of their name.



USER NAME	EMAIL	LABEL
OD Olivia Disco	olivia[redacted]	ADMIN
LS Livvy Sings	livvy[redacted]	USER

If you are an Admin, we will require verification from another Admin in your DISCO.

If you are the only Admin in your DISCO, we will use other means to verify your request.

Frequently Asked Questions

Do I have to use Google Authenticator? Can I use another app?

Our MFA system is compatible with other authenticator apps, such as Okta Verify, Authy, Lastpass, and Microsoft Authenticator. We suggest checking with your IT team to see what they recommend.

I have Google Authenticator set up, but my code isn't working.

Each code is only valid for about 30 seconds. Make sure to enter the code quickly, before a new code is generated. If you continue to have problems, please contact our Support team.

What if I'm a member of more than one DISCO?

Provided you are using the same email account to login, you can use the same MFA codes for any DISCO you are a member of. Note that you will only be prompted for an MFA code on the DISCO's that have the MFA requirement enabled.

MFA is enabled on our DISCO, but I'm using DISCO and it hasn't prompted me to set it up yet.

To prevent disruption in your workflow, you will be prompted to set up MFA the first time you log in after it has been enabled on your DISCO. If you'd like to set it up immediately, please log out and log back in.