Setting up and using Multi-factor Authentication (MFA)

Last Modified on 10/15/2026 1:23 pm PDT

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

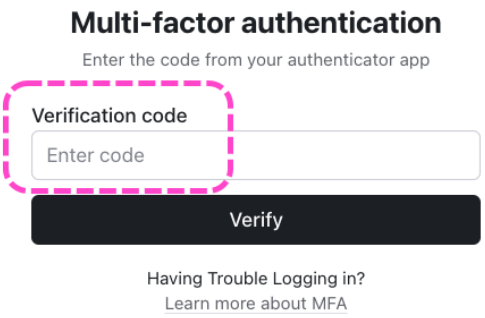
What is MFA?

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 which is usually generated by a third-party authentication app, such as **Google Authenticator**, **Microsoft Authenticator**, **1Password**, 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.

At a glance

If **MFA** is enabled on your DISCO account, you'll need to enter a dynamic six-digit verification code when logging in (after entering your username and password).



These codes *must* be generated by a third-party authentication app of your choice (e.g. **Google Authenticator**).

> ***Note:*** *DISCO does not currently support MFA via SMS.*

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 on a single DISCO, any users belonging to that particular DISCO*

will also be prompted to use MFA when logging in to other DISCOs as well, so long as they're using the same email address to log in to all of their DISCO accounts.

Setting up multi-factor authentication

Pre-requisite steps

Before beginning the setup process, you will need to:

Choose an authentication device

You can use a mobile device or computer.

Choose and install an authentication app or extension

On mobile:

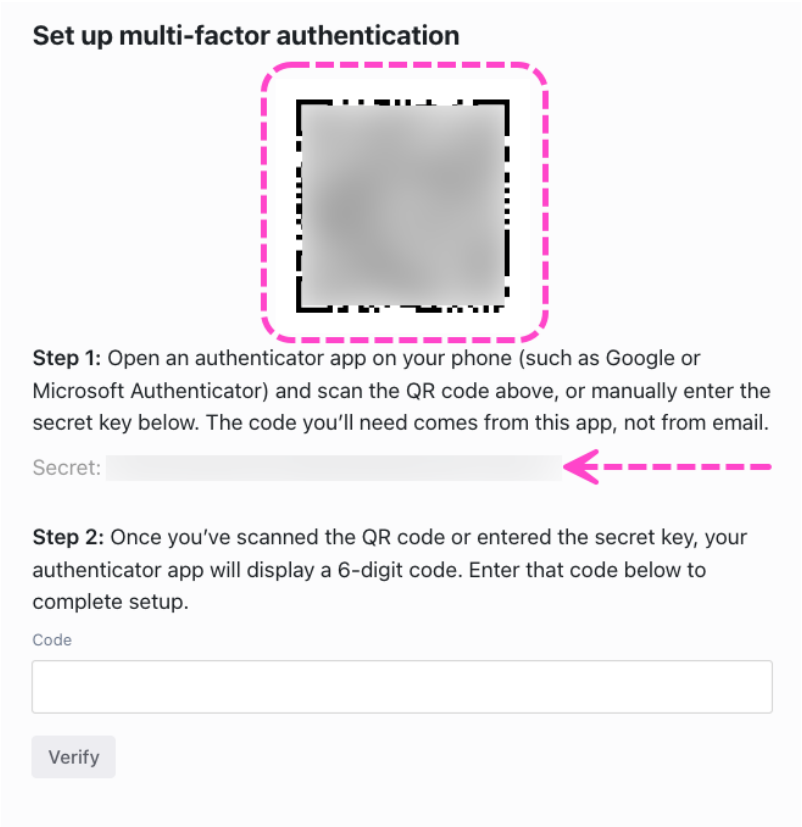
You can install an authentication app from the Google Play Store (Android) or App Store (iOS). Two well-known authenticator apps are **Google Authenticator** and **Microsoft Authenticator**, but any authenticator app will do.

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.

Initial setup

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



The prompt will contain a **QR code** and **Secret** (otherwise known as a "Secret Key") that is *unique to you*. Each individual user on DISCO has their own unique **Secret**.

> ***Note:*** *The screenshots in this article are for demonstration purposes only. You must use the specific* ***QR code*** *and* ***Secret*** *from the prompt in your own DISCO.*

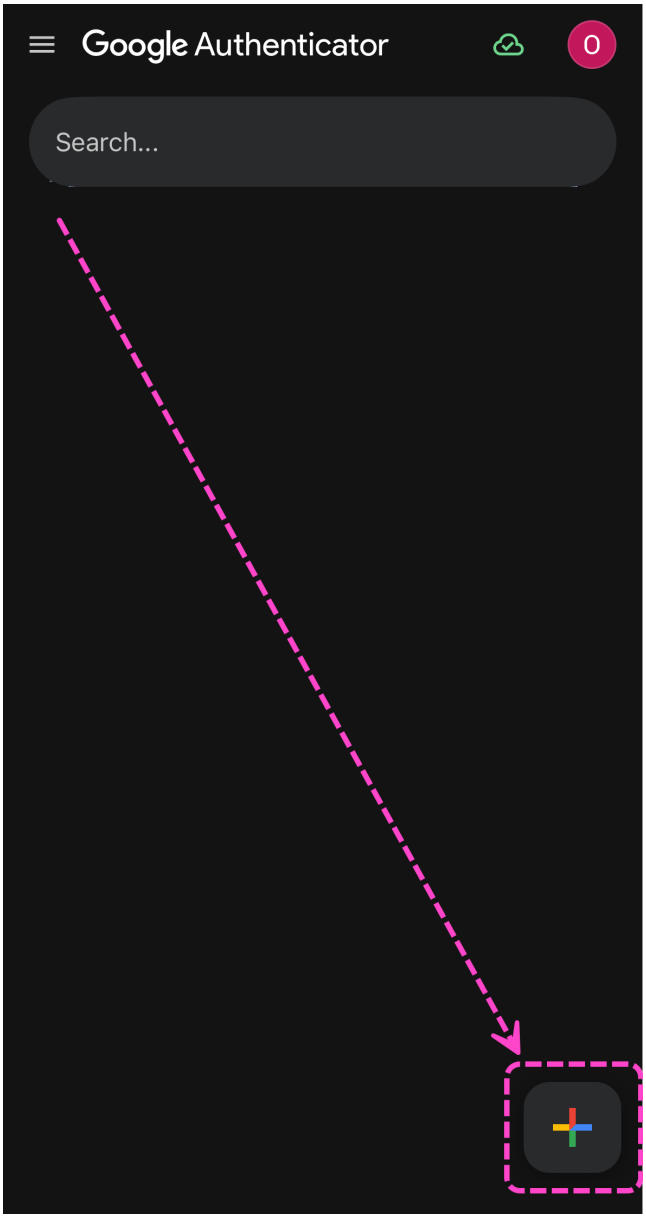
> ***Important:*** *Keep your* ***Secret*** *in a safe place and do not share it with anyone. It will come in handy if you ever lose your authentication device, or lose access to your authenticator app, as you will need it to set up MFA again on another device/app.*

Step 1: Add your DISCO account to your authenticator app

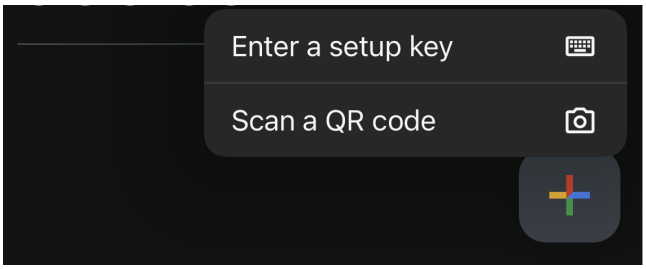
For the sake of simplicity, we have provided instructions below using two well-known authenticator apps: Google Authenticator and **Microsoft Authenticator** on a mobile device.

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 corner.

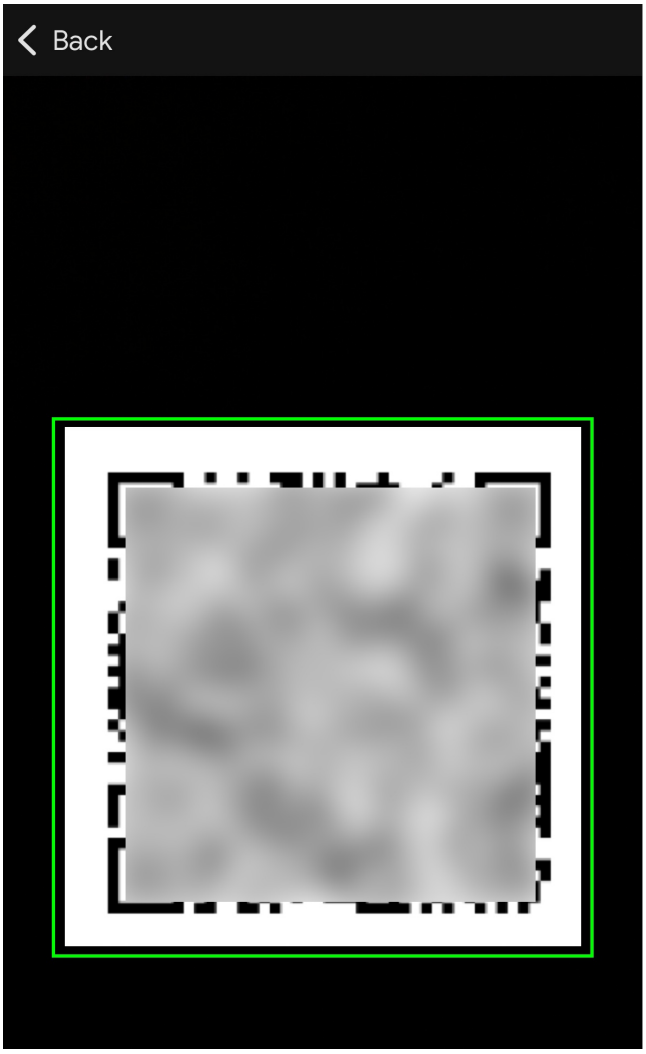


3. Tap **Scan a QR code***. This will open up your camera in barcode scanning mode.

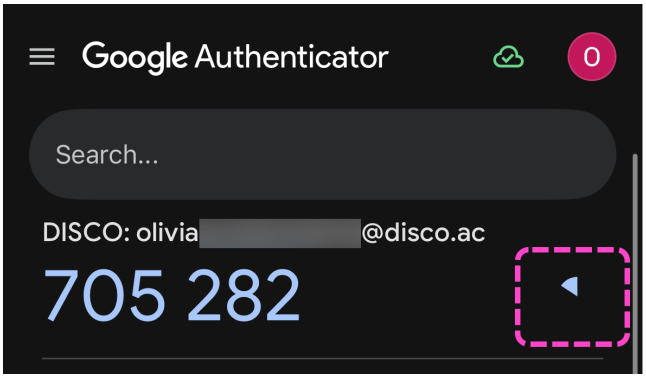


Alternatively, you can tap **Enter a setup key, and enter the **Secret** from the prompt in your DISCO.*

4. If using the QR code option, 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 added to the list automatically for your DISCO account. It will contain a six-digit code that will be valid for 30 seconds until it is replaced by another code, and so on. The timer to the right of the code (that looks like a pie chart) indicates when the code is about to expire.

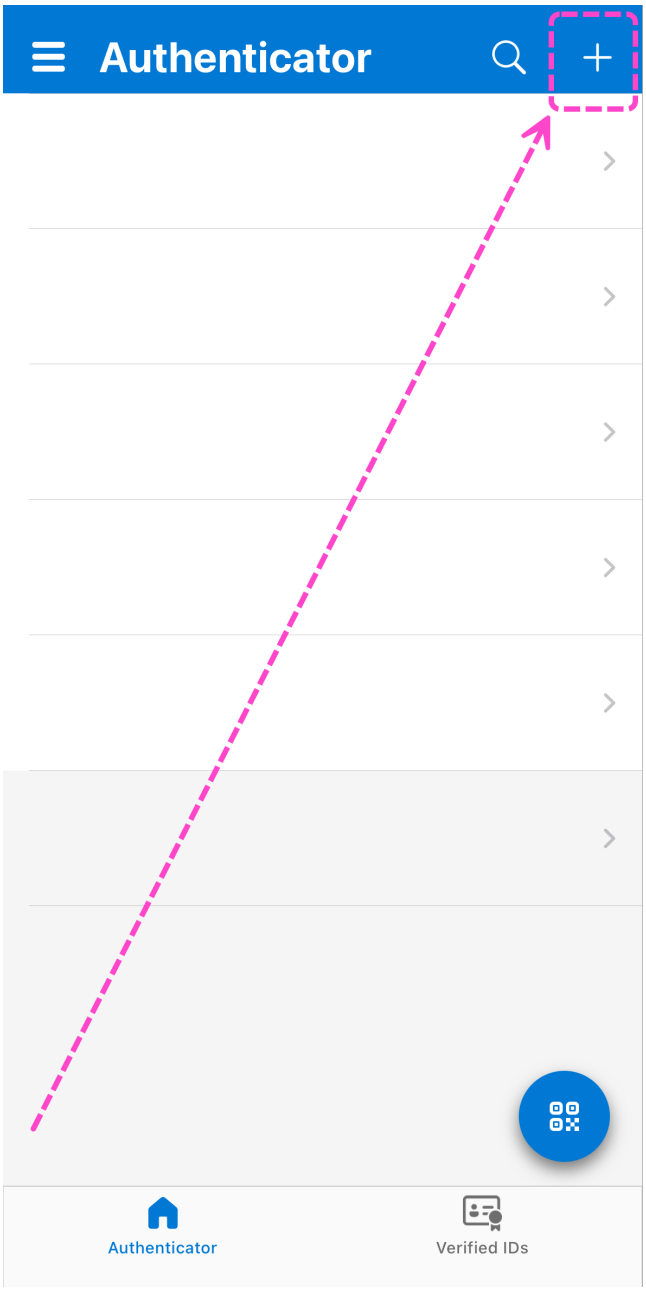


Note: *The screenshots in this article are for demonstration purposes only. You must use the specific codes from your own authenticator app.*

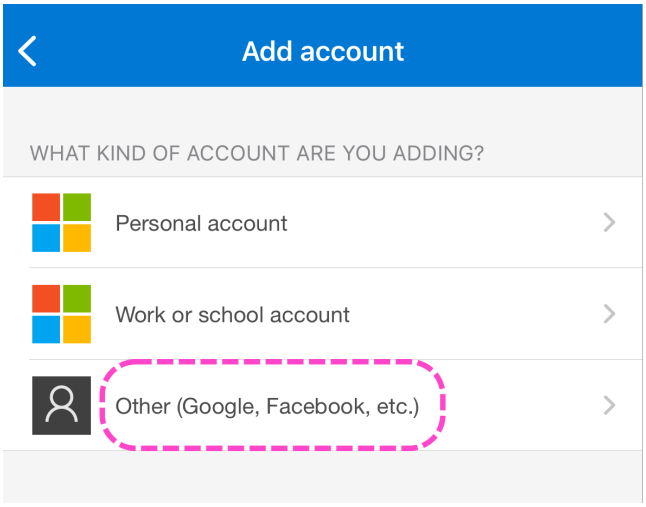
Tip: *If the code turns red, it is about to expire. It's best to wait for the next code to appear to avoid an error message in your DISCO.*

Using Microsoft Authenticator on a mobile device

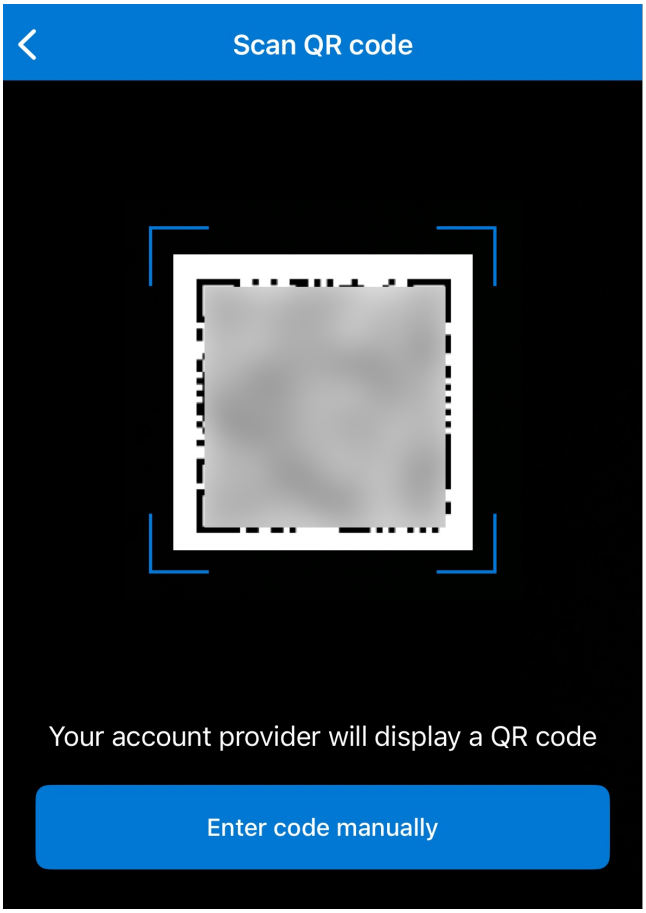
1. Open the Microsoft Authenticator app on your mobile device.
2. To add a new account, tap the **+ plus** icon on the top right corner.



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

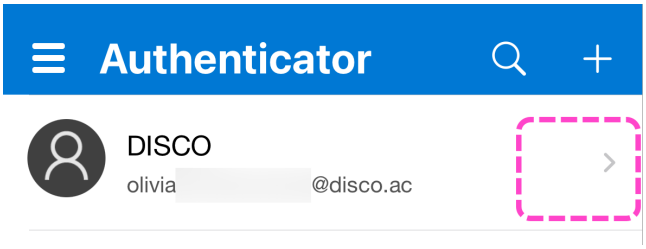


4. This will open up your camera in barcode scanning mode*.
5. Hold your mobile device up to your computer screen, with the QR code centered in your camera.

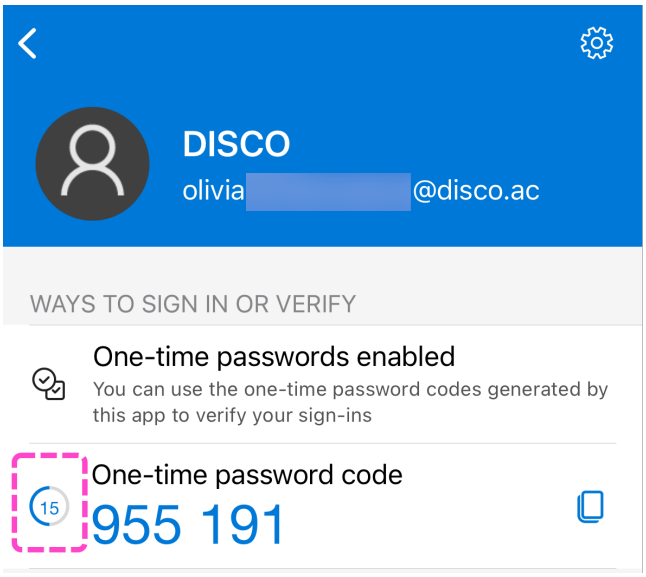


Alternatively, you can tap **Enter code manually, and enter the **Secret** from the prompt in your DISCO.*

6. A new entry will be created for your DISCO account. Tap on it to reveal the code.

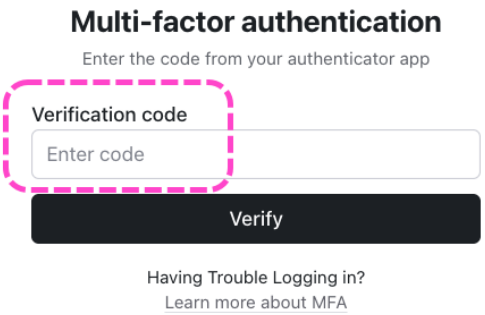


7. The code will be valid for 30 seconds until it is replaced by another code, and so on. The timer to the left of the code indicates when the code will expire.



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

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



After you've logged in, a message will appear in the bottom left corner of your DISCO to confirm MFA has been activated:



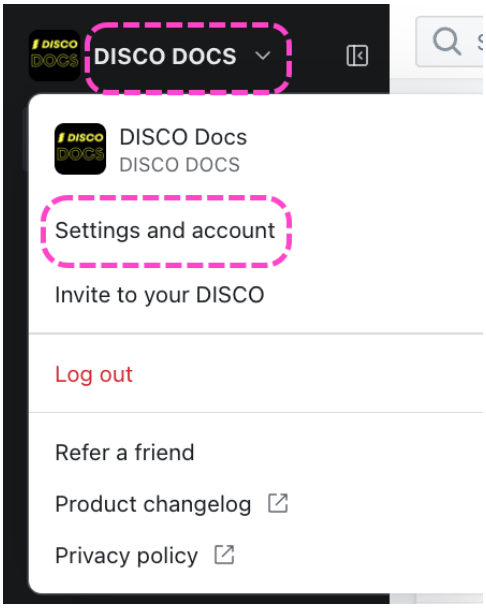
> ***Note:*** *Now that MFA is successfully enabled on your DISCO, you'll be prompted to enter a six-digit code each time you log in.*

Resetting multi-factor authentication

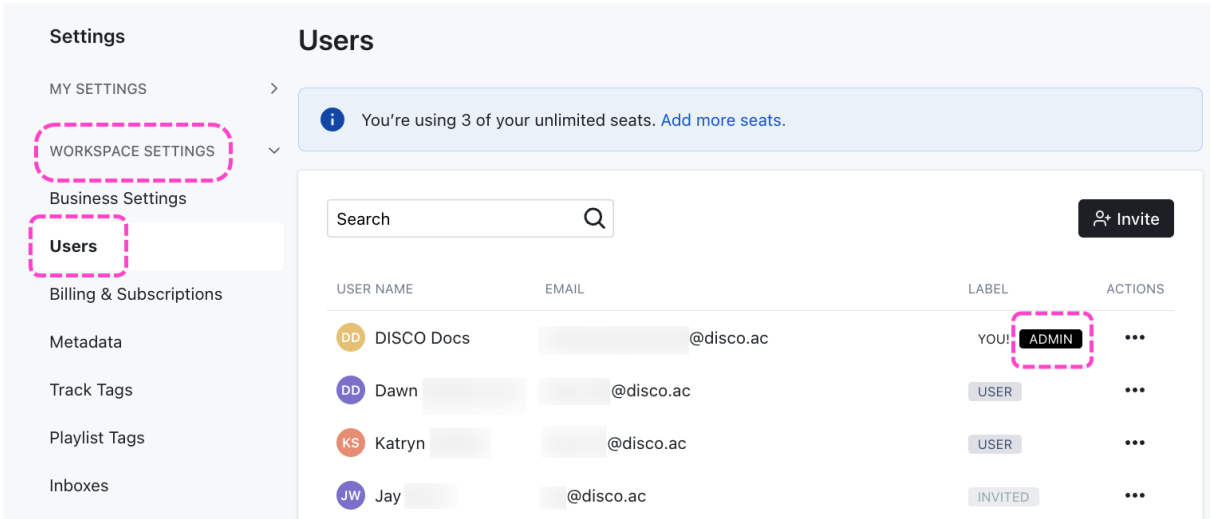
If you no longer have access to the device or authenticator app you set up MFA with, or if you need to set up a new device/app, your MFA credentials must be reset. In any case, for security purposes, you will need to send an email to our Support team at support@disco.ac.

We will require verification from one of the Admins on your account, so to expedite this, 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 the **Account Switcher** (your DISCO Business Name) and select **Settings and account**.



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



> ***Notes:***
>
> - *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.