Configure 2-Factor Authentication (2FA)

Last Modified on 27.11.2023

What it is

2-Factor Authentication (2FA) is an additional security layer in the login flow for Userlane Manager Users. Once enabled, Managers will be prompted to configure 2FA with their Authenticator App of choice.

They will then need to enter an authentication code after providing their username and password to access the Userlane Portal.

Why use 2FA

There are 3 commonly accepted Authentication Factors:

1. Knowledge: Something you know, like a password.
2. Possession: Something you have, like a smartphone with an authenticator app.
3. Inherent: Something you are, like your fingerprint or faceID.

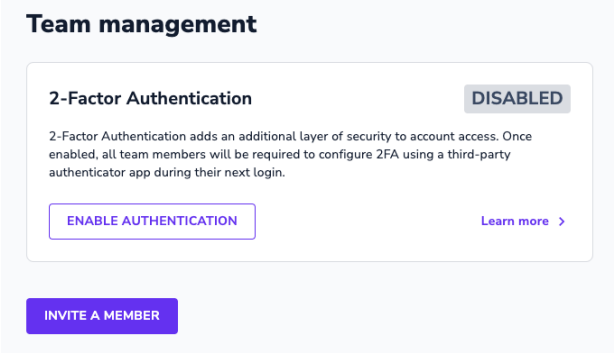
2-Factor Authentication requires the use of two of the above three authentication factors for login. At Userlane, the two authentication factors needed are **Knowledge** (your password associated with your email address) and **Possession** (the Authentication Code generated by your authenticator app).

Userlane 2FA supports the use of the following 3 authenticator apps:

- **Microsoft Authenticator**
- **Google Authenticator**
- **FreeOTP**

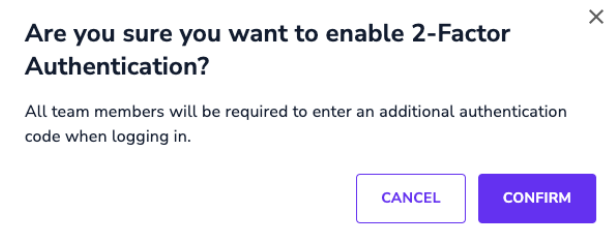
How to Enable 2FA

On the Team Management page in the Userlane Portal, Managers with the Admin Role will see the option to enable 2FA for all Team Members in their Userlane company.



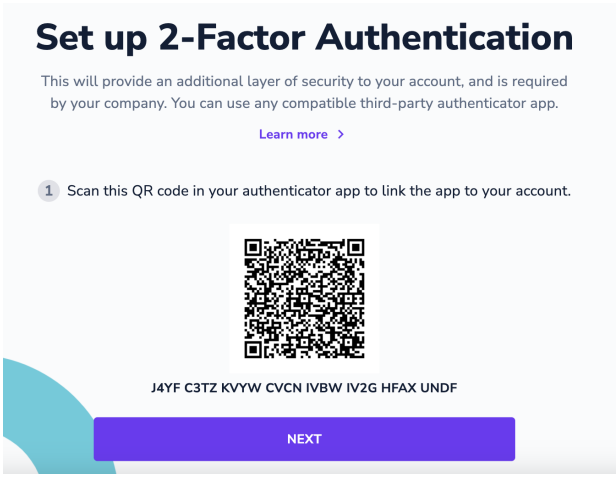
After clicking ‘Enable Authentication’, Admins will be asked to confirm that they want 2FA enabled for their

Team Members.

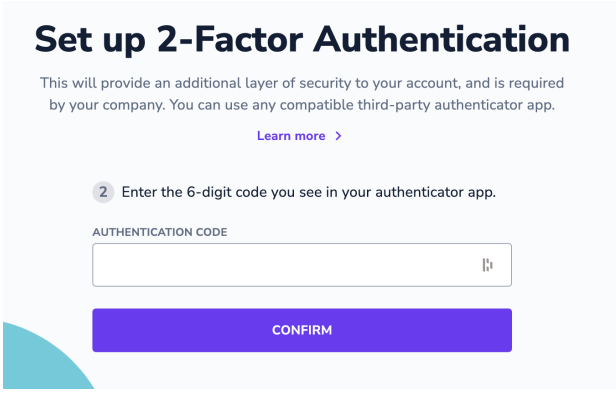


How to Set Up 2FA

Once enabled, all Team Members in that company will be prompted to set up 2FA during their **next log-in** to the Userlane Portal. After entering their username and password they will be prompted with:

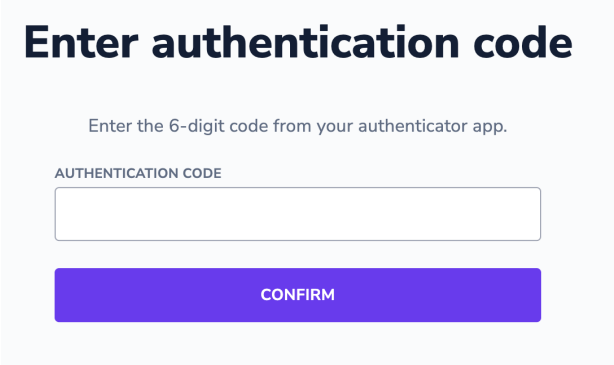


Userlane Managers will then need to configure 2FA with their preferred authenticator app by scanning the QR code with their app or manually entering the alphanumeric code. They will then be prompted to enter their authentication code in order to complete the login process.



Note: if you accidentally enter the code incorrectly when setting up 2FA, you will be prompted to scan the QR code again in order to generate a new authentication code for set up.

Once enabled and configured, managers will be prompted to enter their authentication code every time they log in to the Userlane Portal as shown below.



Disabling and Resetting 2FA

Admin Users can also disable 2FA for all Team Members in their organization or reset the 2FA configuration process for individual team members, for example, in case a User has lost the phone they used to configure 2FA with an Authenticator App. These settings can also be found on the Team Management page.