Two-factor Authentication

Last modified on: 08/06/2025 3:03 pm MST
Tags: Keap-Pro Keap-Max Max-Classic Keap-Ultimate

As of August 7, 2025, two-factor authentication (2FA) is required for all Keap users, including partners who manage client accounts. This change enhances security and helps protect access to Keap apps from unauthorized use. Two-factor authentication significantly enhances the security of your account by requiring two different forms of identification. This helps protect against common threats such as password breaches, phishing attacks, and unauthorized access, providing you with a more secure experience.

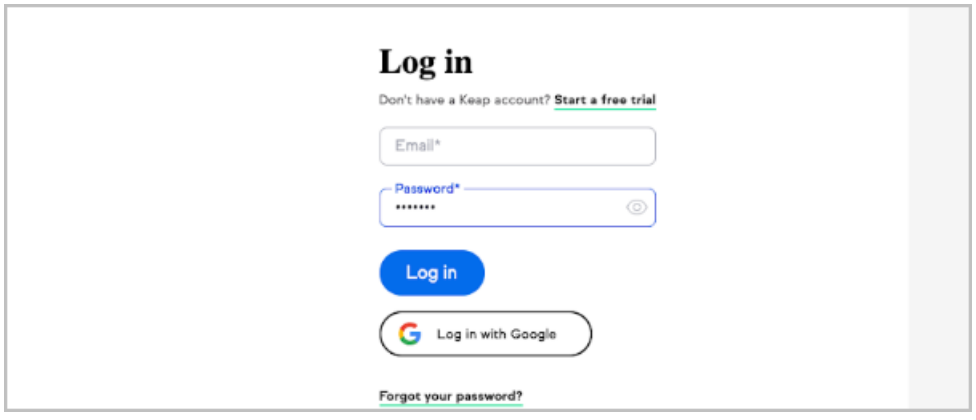
You will be required to enable 2FA at next login if not already configured.

You won't be re-challenged by 2FA for 90 days after your most recent challenge or unless a new device attempts to access the account.

You're likely already familiar with Two-Factor Authentication (2FA) in other online software applications. Soft 2FA, also known as software-based 2FA, uses software applications on your device to generate one-time passwords (OTPs) for logins. Once set up, you won't be re-challenged by 2FA for 90 days after your most recent challenge or unless a new device attempts to access the account. Here's how it will work:

Email 2FA

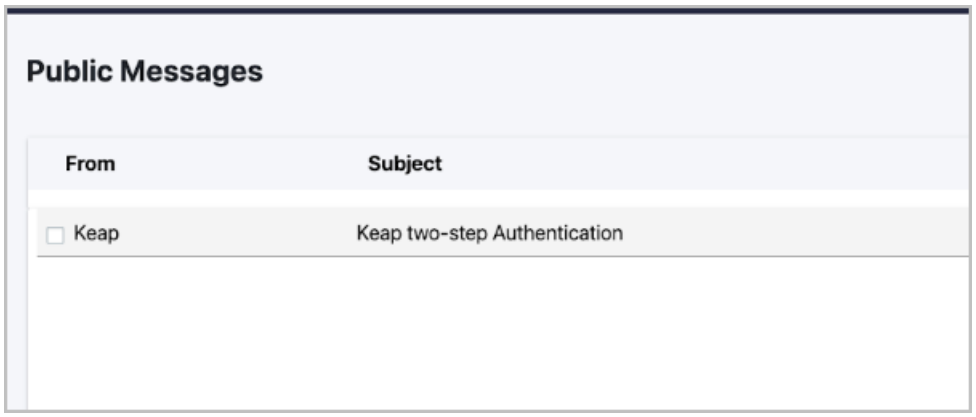
1. Enter your username and password on the login page as usual



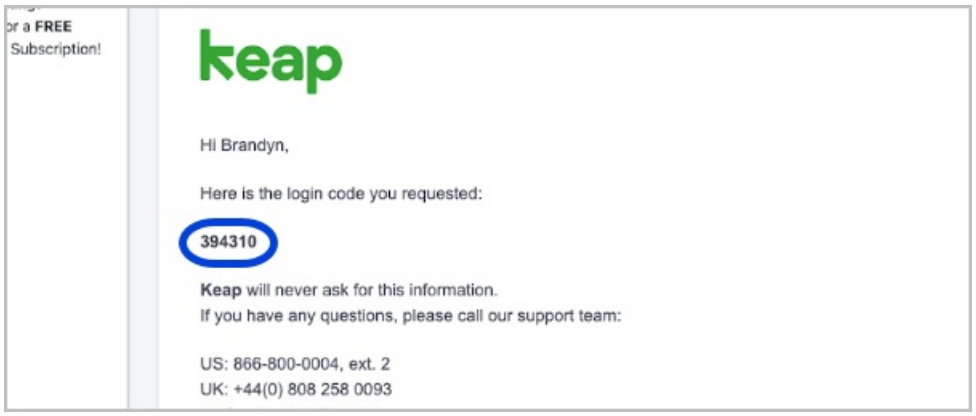
2. If you haven't set up 2FA, you will be prompted to enter a “One Time Password” that will be sent to your email.

3. Navigate to your email inbox.

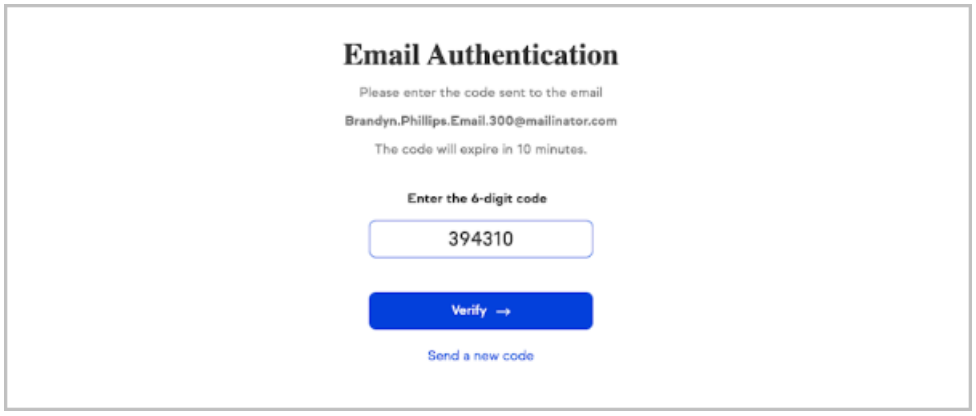
4. Look for an email from Keap titled **Keap 2-step authentication**.



5. Retrieve the six-digit code from the email.



6. Enter the code on the challenge page.



7. Click **Verify** to continue or **Send a new code** if you did not receive one.

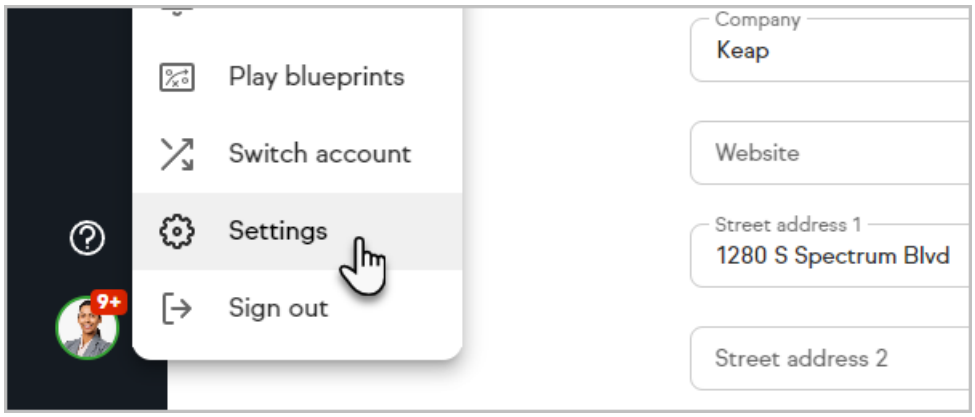
8. If you are unable to receive the code or no longer have access to the email on file, contact Keap support for assistance.

9. Once you successfully pass the challenge, you will be navigated to your dashboard and can continue using the application as usual.

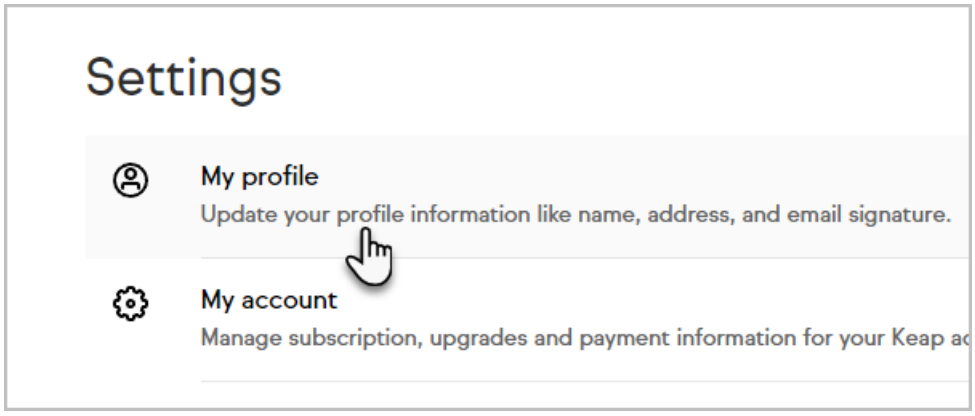
Switching to Text 2FA

If you prefer to use your mobile phone to receive the authentication code, please follow these steps:

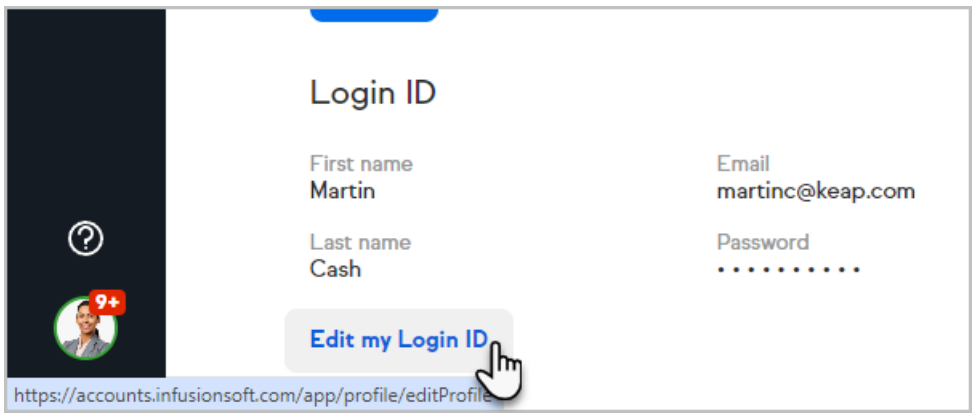
1. Go to the Security Settings page in **Account Central**.
    a. For Keap Pro, Ultimate, and Max, click on your user icon and select**Settings**



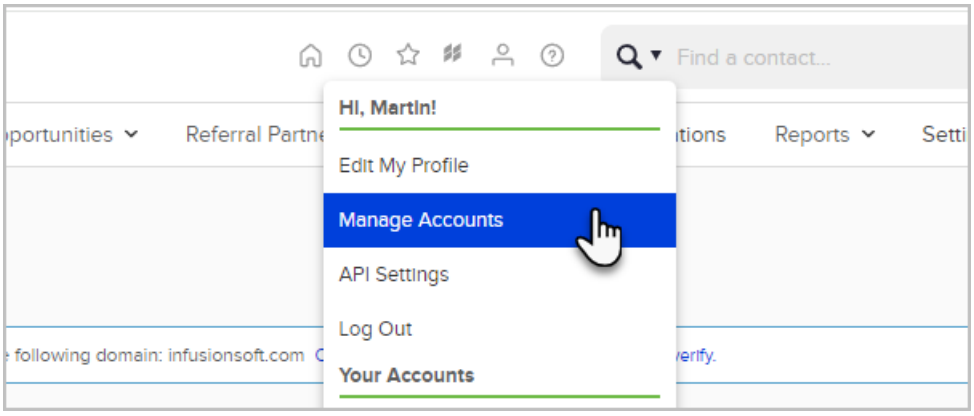
    b. Click **My profile**



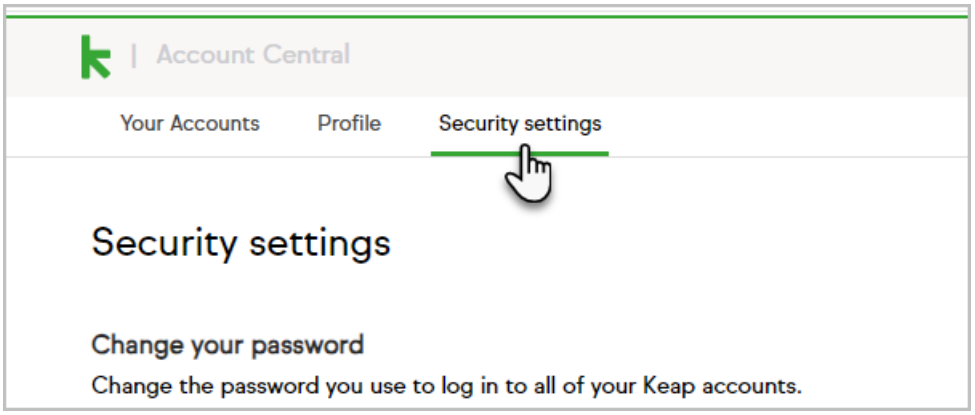
    c. Scroll down and select **Edit my Login ID**



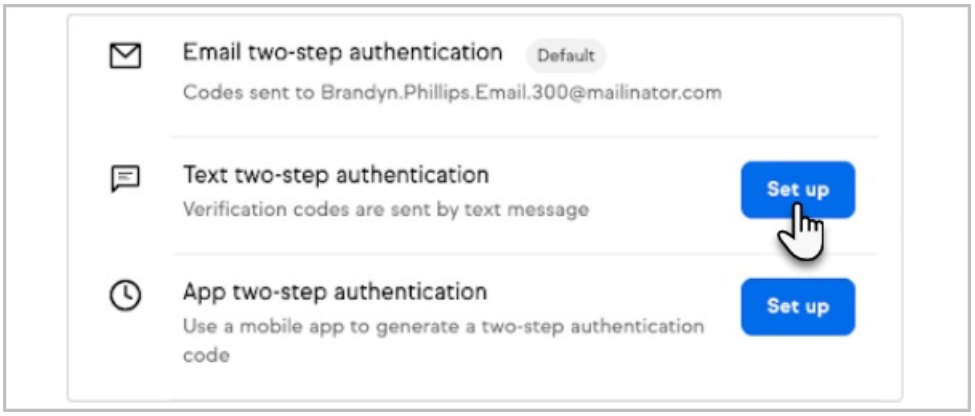
    d. For Max Classic users, click on the person icon and choose, **Manage Accounts**



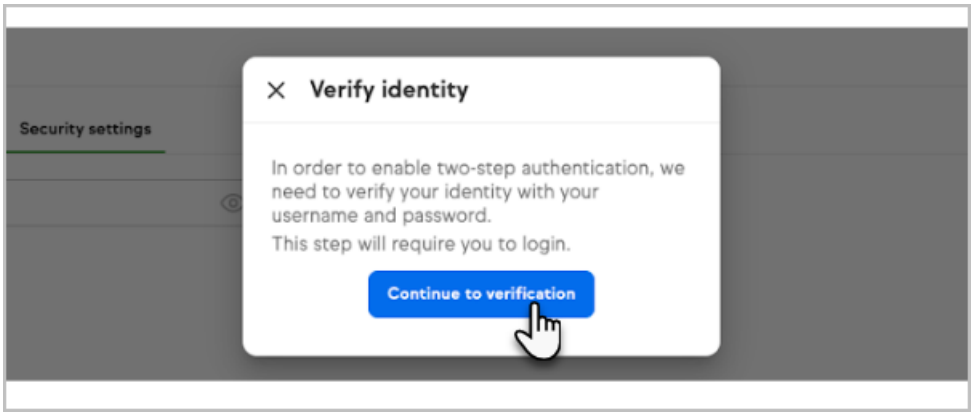
2. Choose **Security settings**



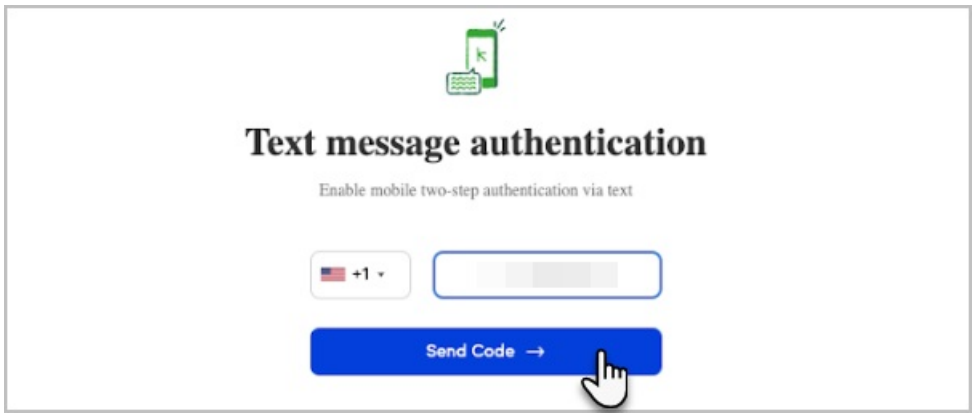
3. Under the **Two-step authentication** section, click **Set up** next to the **Text two-step authentication** option



4. Click **Continue to verification**.



5. Enter the desired phone number that will be used in Text 2FA and click **Send code**



6. Retrieve the six-digit code from your mobile device and verify your code on the challenge page.

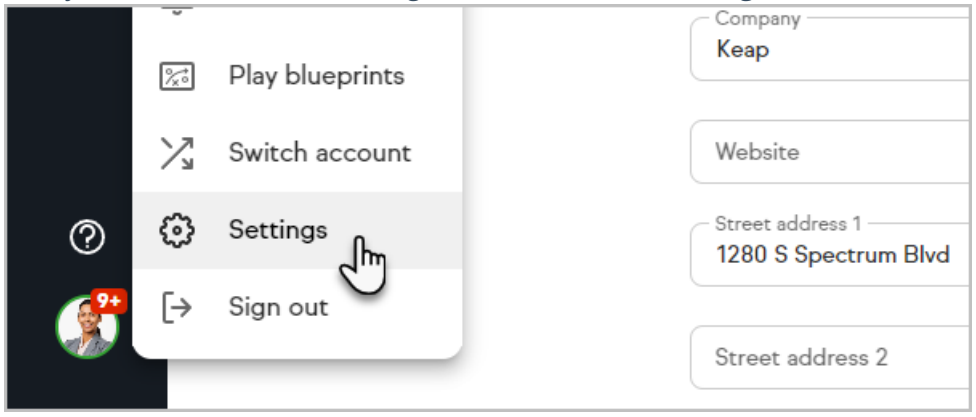
7. Once verified via login credentials, text 2FA will be your primary form of authentication!

Switching to App-Based 2FA Authenticator

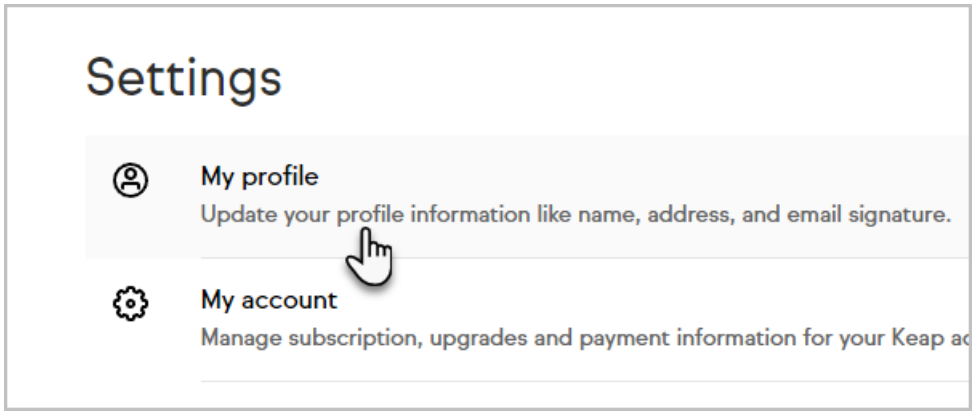
If you prefer to use an authenticator app (like Google Authenticator, Microsoft Authenticator, or Authy) instead of text message codes, follow the steps below

For Keap Pro, Ultimate, and Max users:

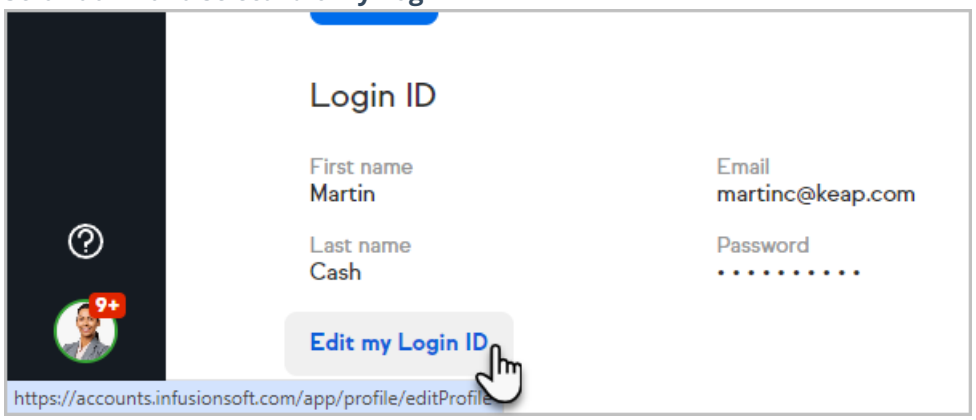
1. Click your user icon in the lower right corner and select **Settings**



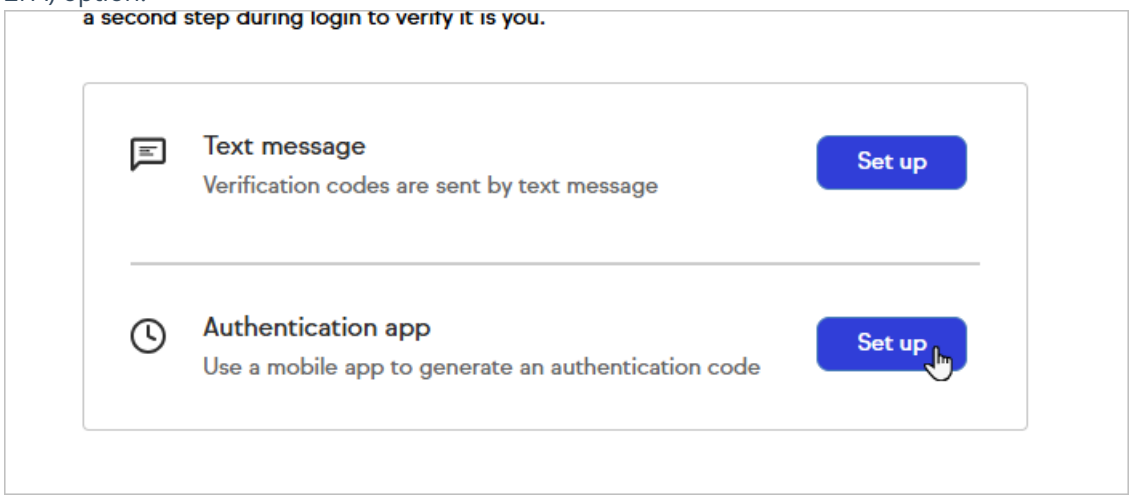
2. Then click **My profile**



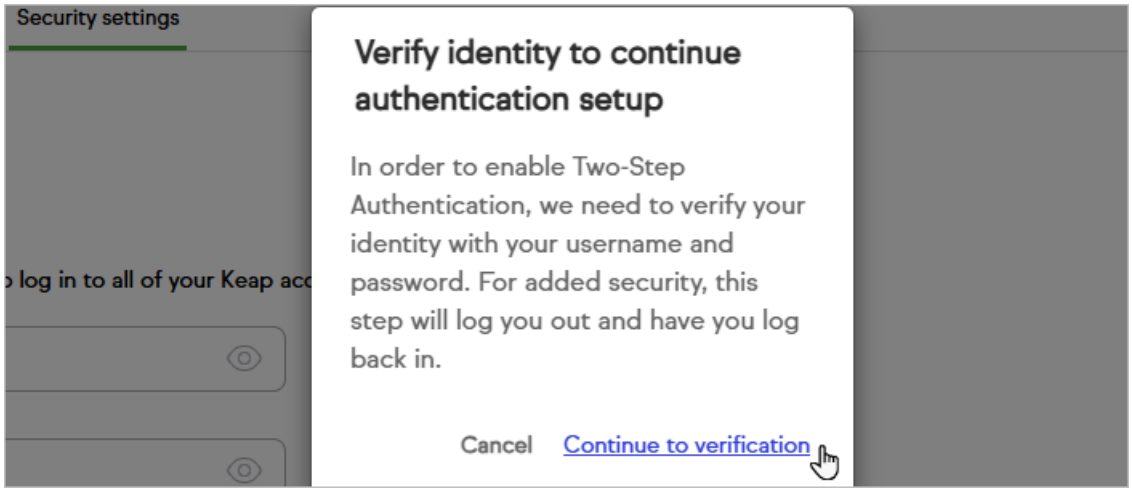
3. Scroll down and select **Edit my Login ID**



4. Under the Two-step authentication section, click **Set up** next to the **Authenticator App** (App-based 2FA) option.



5. Click **Continue to verification**

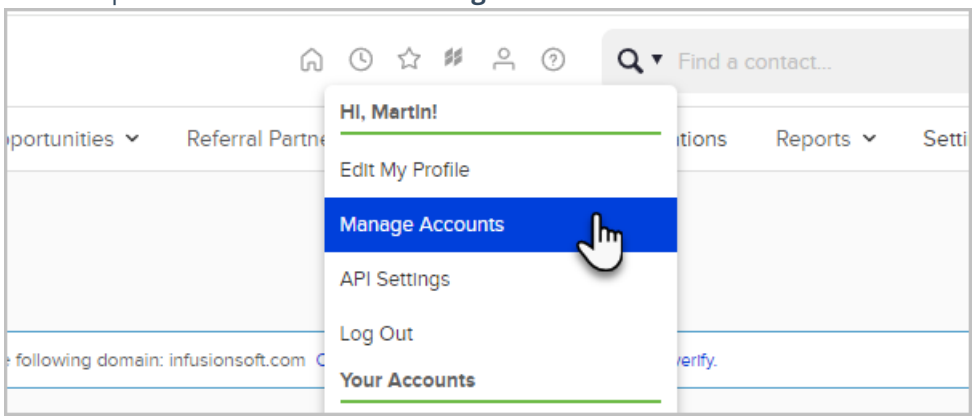


6. On the setup screen, you'll see a QR code

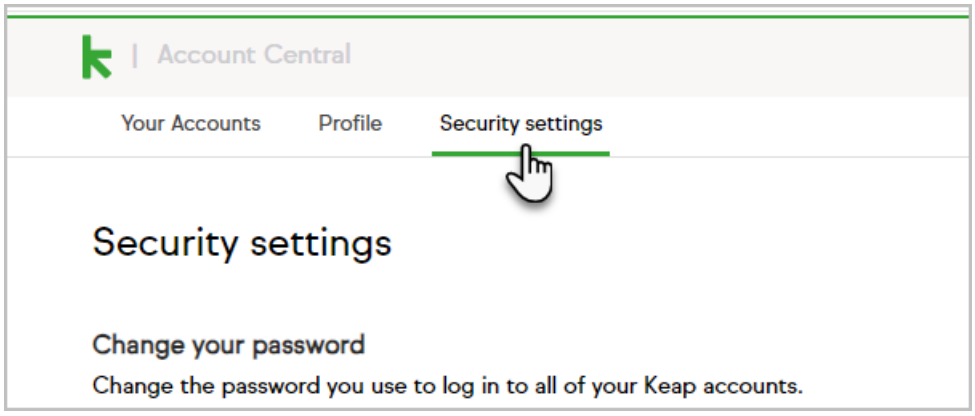
7. Open your authenticator app (e.g., Google Authenticator or Authy) and scan the QR code.Your app will generate a 6-digit code — enter that code on the challenge page to complete verification.Once verified, App-based 2FA will be your primary form of authentication going forward.

For Max Classic users:

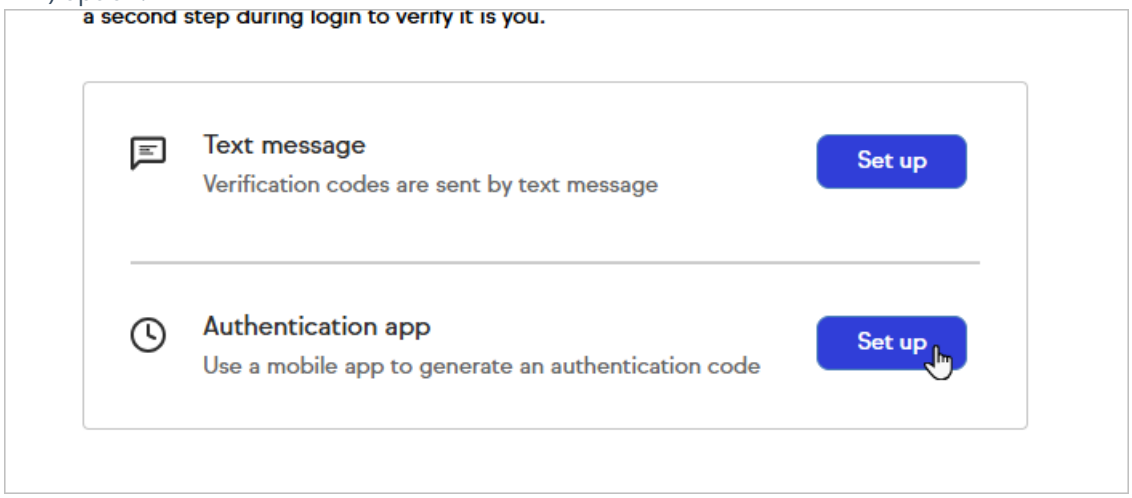
1. Click the person icon and choose **Manage Accounts**



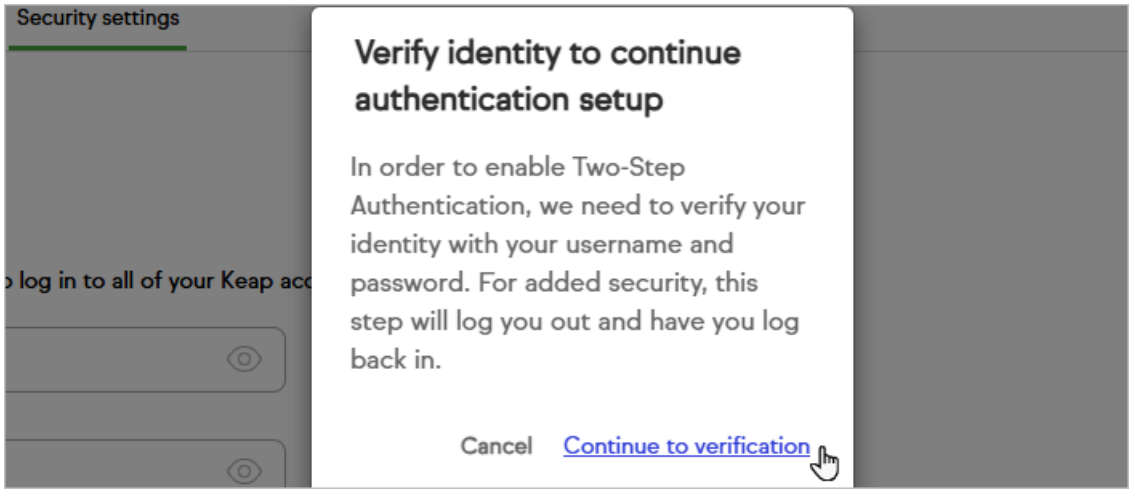
2. Choose **Security settings**



3. Under the Two-step authentication section, click **Set up** next to the **Authenticator App** (App-based 2FA) option.



4. Click **Continue to verification**

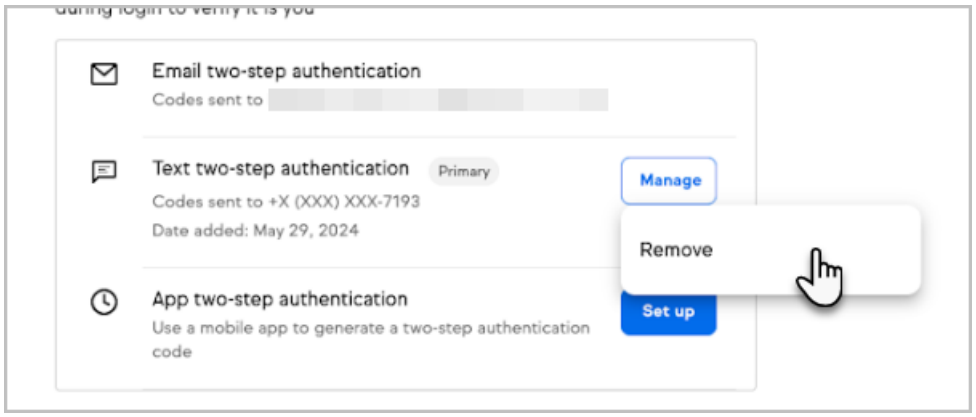


5. On the setup screen, you'll see a QR code

6. Open your authenticator app (e.g., Google Authenticator or Authy) and scan the QR code.
7. Your app will generate a 6-digit code — enter that code on the challenge page to complete verification.
8. Once verified, App-based 2FA will be your primary form of authentication going forward.

Switch back to email 2FA

1. Remove the previously configured text 2FA option.



Important Notes

- Mandatory 2FA requires at least email 2FA to be enabled at all times. Removal of all 2FA methods is not allowed.
- Re-challenge Interval: You won't be re-challenged by 2FA for 90 days after your most recent challenge or unless a new device attempts to access the account.
- Verified devices can be viewed and removed in Account Central under the Security settings page.