Setting Up Multi-factor Authentication (MFA) Using Google Authenticator

Within your EP products multi-factor authentication (MFA) may be required. MFA is a one-time passcode you enter each time you sign in to help keep your information protected.

If you have been prompted to set up your MFA when you sign in to your EP products, below is an overview of the process if you choose to use Google Authenticator.

Getting started:

Download the app: **To complete MFA using Google Authenticator, download and install the Google Authenticator app to your mobile device.** You can get the app from the App Store for iPhone or the Play Store for Android. (You can also download and use Authy desktop/mobile, Duo, or Okta Verify but they are not covered in these guides.)

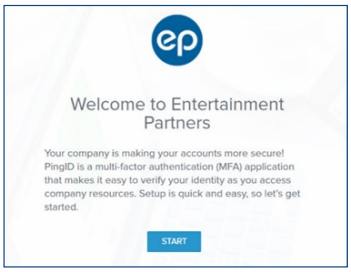
Download on the App Store

GET IT ON Google Play

STEP 1

Steps to set up:

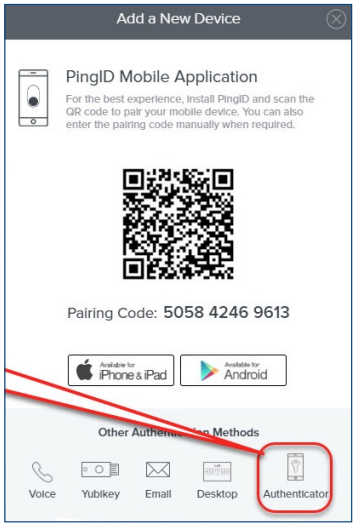
1. Sign in to your EP product with your username and password. You'll be taken to the Welcome multi-factor authentication screen. Click **START**.



Setting Up Multi-factor Authentication (MFA) Using Google Authenticator (Continued)

STEP 2

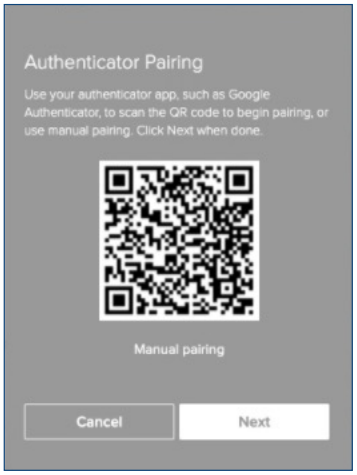
2. The Add a New Device screen opens. DO NOT scan the QR code. Instead select **Authenticator** in the lower right corner.



STEP 3

3. From your mobile device, open the Google Authenticator app (or the authentication app of your choice.) Scan the QR code. Once you scan the QR code, the passcode displays.

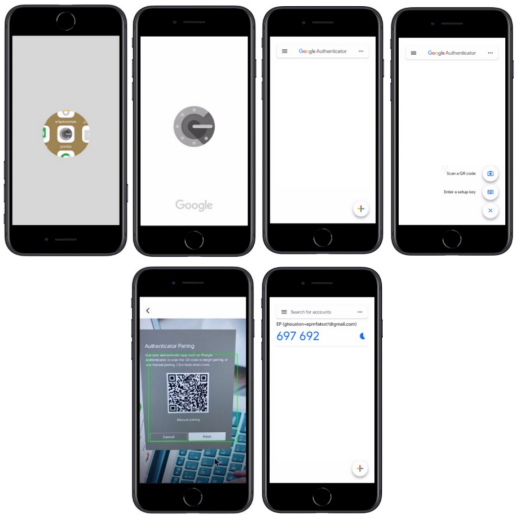
If you can't scan the QR code, enter the 12-digit Pairing Code.



Setting Up Multi-factor Authentication (MFA) Using Google Authenticator (Continued)

STEP 4

4. Then, click **Next** on the Authenticator Pairing screen. Enter the Google Authenticator passcode (or passcode from another authentication app) into the Verification screen.



STEP 5

5. Click **Next** on the Verification screen to complete. You can now use Google Authenticator or other authentication app for your one-time passcode to access your EP products.