MYAPPS (OKTA) GOOGLE AUTHENTICATOR ENROLLMENT

The **Google Authenticator** will generate a numeric token on your mobile device to enter into MyApps on your desktop as an additional login factor, only when you are using applications managed via MyApps or the application being accessed is considered high-risk. Use of the Google Authenticator mobile application will ensure that WEX is following industry-mandatory security practices for Multi-Factor Authentication (MFA). This additional factor will prompt you to setup and provide a token code

---

First time set up of Google Authenticator on a Mobile Phone:

1. Login to **MyApps** (https://wexinc.okta.com/app/UserHome)

2. From the top-right menu, select the drop down by your name and then click **Settings**

3. Scroll half way down the settings page to the **Extra Verification** section

4. Click **Setup**
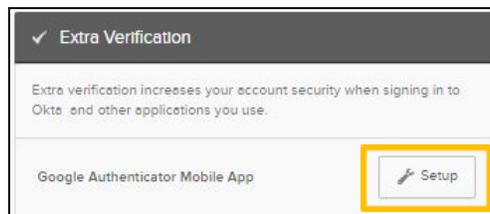
5. Choose the mobile device type you will be using to authenticate your network, then click **Next:**
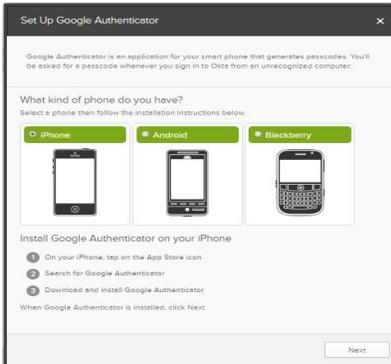
6. **Go to the App Store on your phone**
7. Download the **Google Authenticator** app
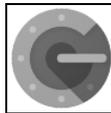
8. Open Google Authenticator on your mobile device.

9. Inside the Google Authentication app, tap **Begin Setup**
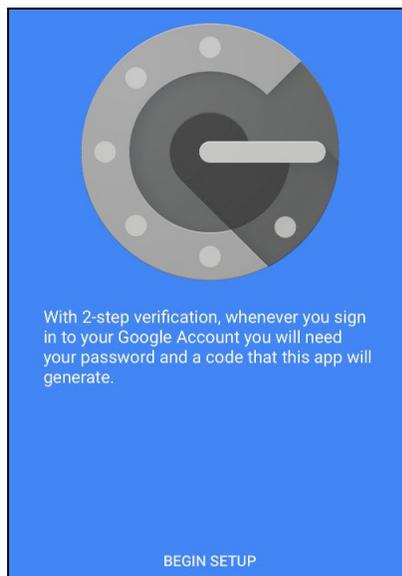
10. Click **Scan Barcode**
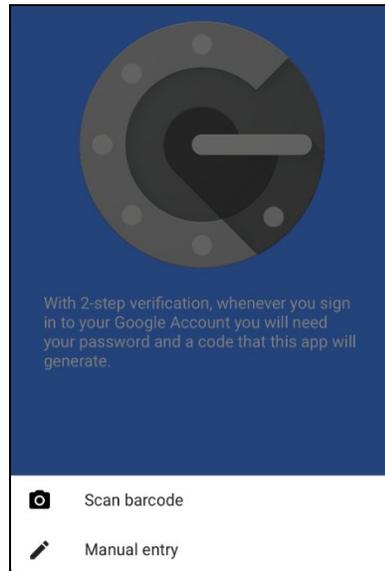
11. Point your mobile device at your computer screen putting the **QR code** supplied by your MyApps portal in focus. The barcode below is just an example.
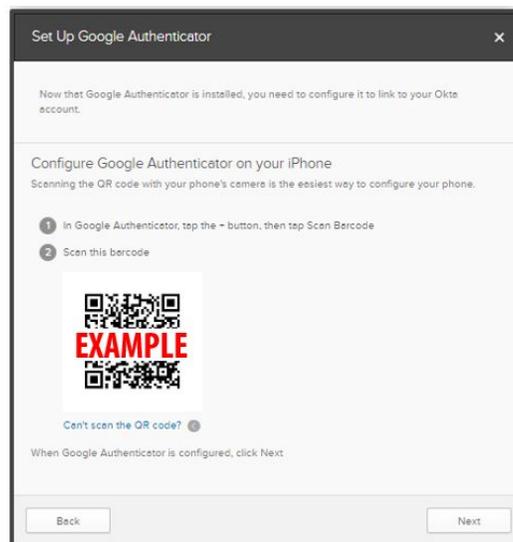
12. After recognizing the code, a **6 digit code** will appear on your phone. Enter this into the field on your computer and click **Verify**.

13. Setup is complete.

Moving forward, you will need to supply a 6 digit code from your Google Authenticator to MyApps in order to access anything managed by the portal, such as Gmail or ADP.