Guidance for Microsoft Authenticator

STEP 1 – SETTING UP MICROSOFT AUTHENTICATOR

- If your phone has biometric authentication, Microsoft Authenticator allows you to log in securely with biometric authentication enabled rather than entering a password every time you login to websites or apps.

- First, **download and open** the Microsoft Authenticator app.

Figure 1: Picture of Microsoft Application icon.

- Launch the **Application**, allow notifications and accept the privacy policy.

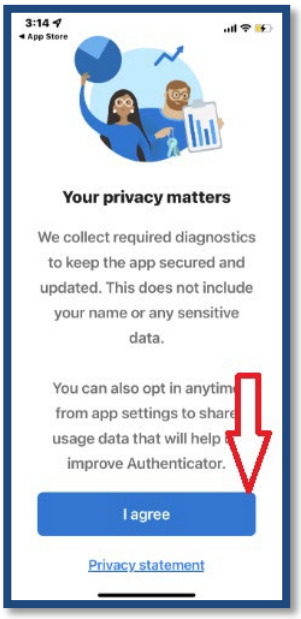

Figure 2: Picture of privacy screen.

- Next, select to **add your SSO account**. Below a couple of different views depending on your Microsoft app version.

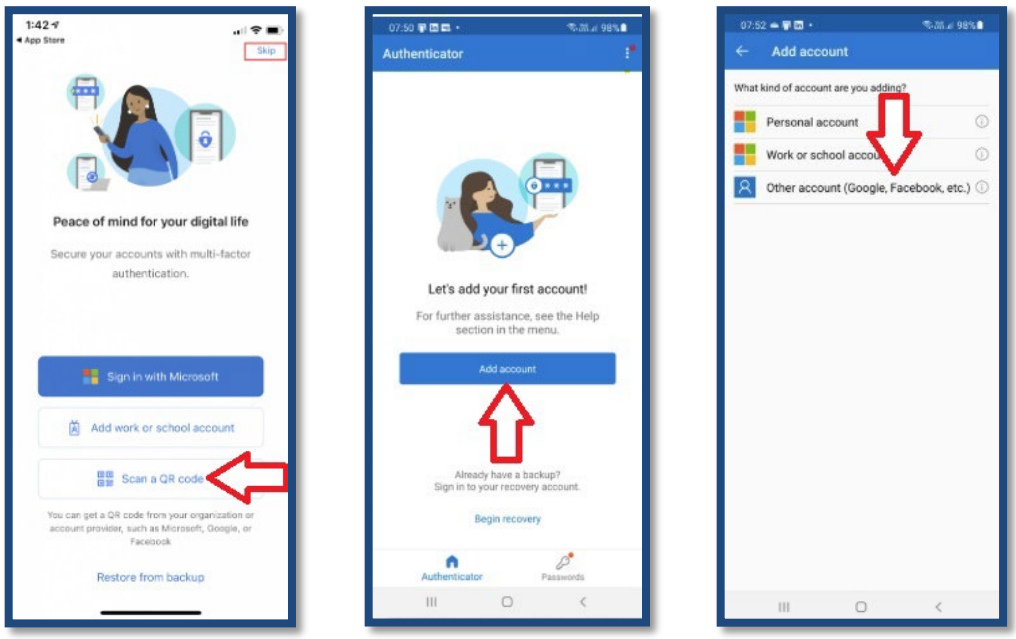

Figure 3: Pictures to add an account.

- You want to select **Scan QR code**, the "**+**" plus sign at the top right of the screen or **other account (Google, Facebook, etc.)**
- A new screen will open to **Scan QR code** or **Enter code manually** by tapping the bottom of the screen to enter the code as the Secret Key (Manual Setup Code on SSO screen).

Figure 4: Picture to scan QR code or enter code manually.

- Finally, aim your phone at your computer to **scan the QR code** or copy and paste the **Manual setup code** provided by SSO onto your phone.

Figure 5: Picture of screen to Setup QR code or enter code manually

- The Microsoft app will immediately add your SSO account, name the account on the app similar to the image below, and provide a 6 six-digit code.

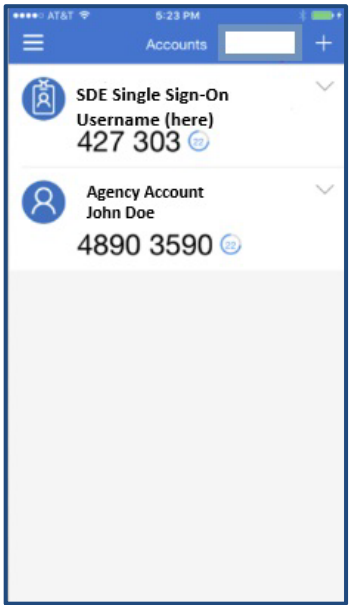

Figure 6: Picture of screen with SSO account successfully added.

- The setup is complete on the Microsoft authenticator application.

Note:

- Available screens and settings may vary by wireless service provider, software version, and phone model.

STEP 2 – COMPLETING THE SETUP ON SSO

- After initial log in to SSO, the following screen will open providing a **QR code** and a **Manual Setup Code**.

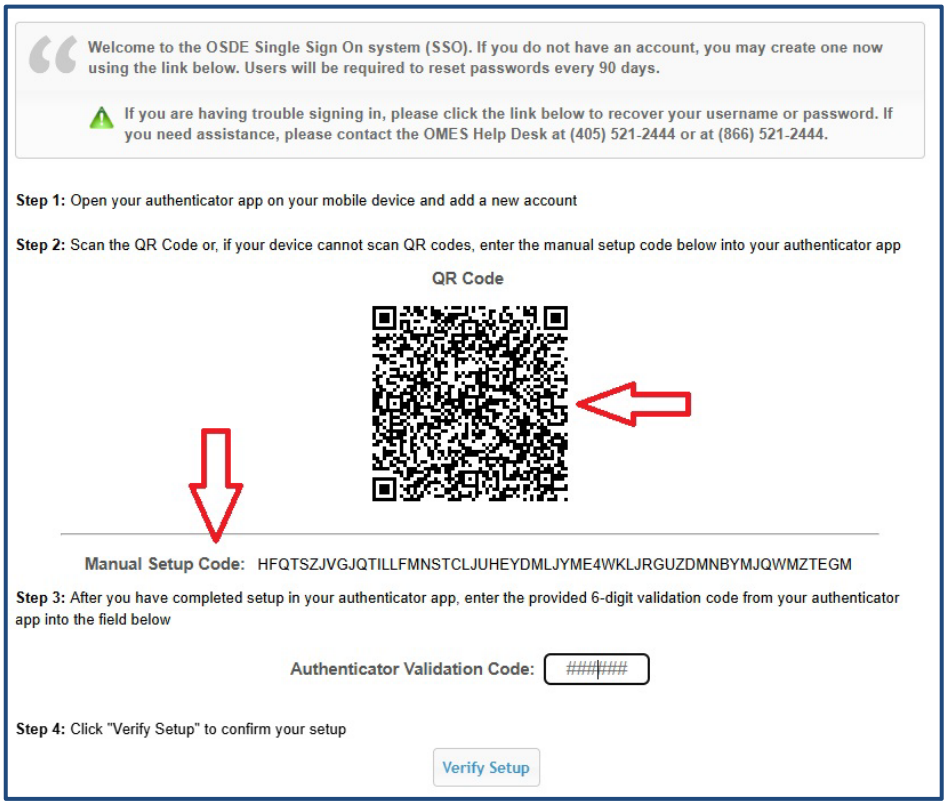

Figure 7: Picture of screen with QR Code and Manual Setup Code

- Either the **QR code** or the **Manual Setup Code** may be used with the Microsoft authenticator application.

- After either code is entered, the Microsoft authenticator application will show a **6 six-digit** verification code. The code expires after approximately 30 seconds, when a new code appears automatically.

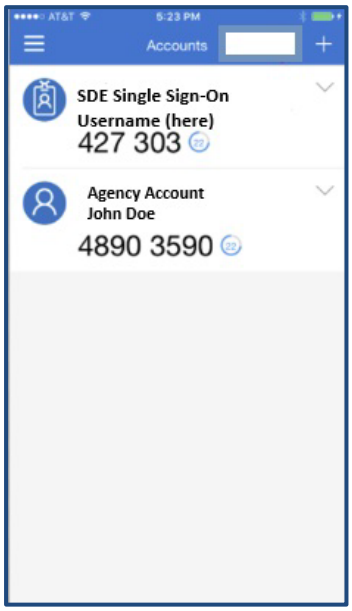

*Figure 8: Picture of screen with 6 six-digit code. **427 303***

- The code is entered in the **Authenticator Validation Code** box pointed in Figure 9 below. Spaces are not needed, only the six digits.

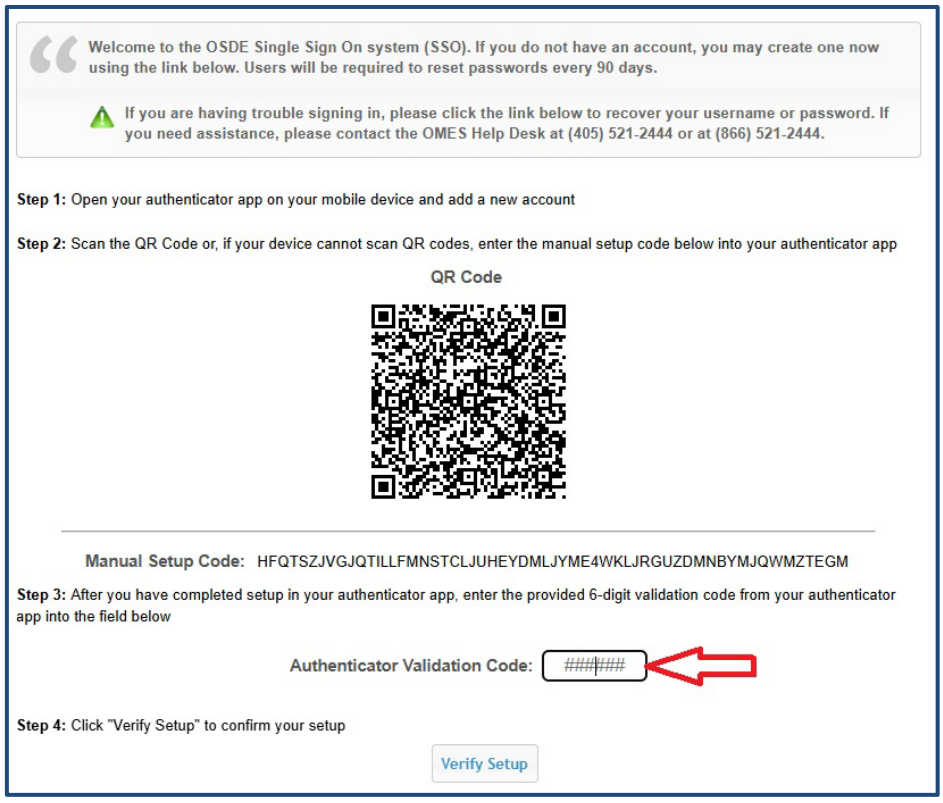

Figure 9: Picture of screen with Authenticator Validation Code box

- The SSO setup is complete.

STEP 3 – LOGGING IN AFTER INITIAL SETUP

- After **SSO username and password** are entered, the screen below will require an **Authenticator Validation Code**.

Figure 10: Picture of subsequent login screen with Authenticator Validation Code box

- You will access the Microsoft authenticator app to retrieve the **6 six-digit validation code** and enter it above.

- These steps are repeated each time for login to SSO or after no activity on your SSO account for an hour.

- Username → password → authenticator validation code.