Keystone Funding's Guide to MFA

Overview: Beginning <mark>November 18th, 2024,</mark> Keystone Funding's B2B Portal, FLEX, will utilize Multi-Factor Authentication to access the system. There are two available options to receive a one-time passcode, Email and Device. By default, the Email option will be selected unless otherwise updated.
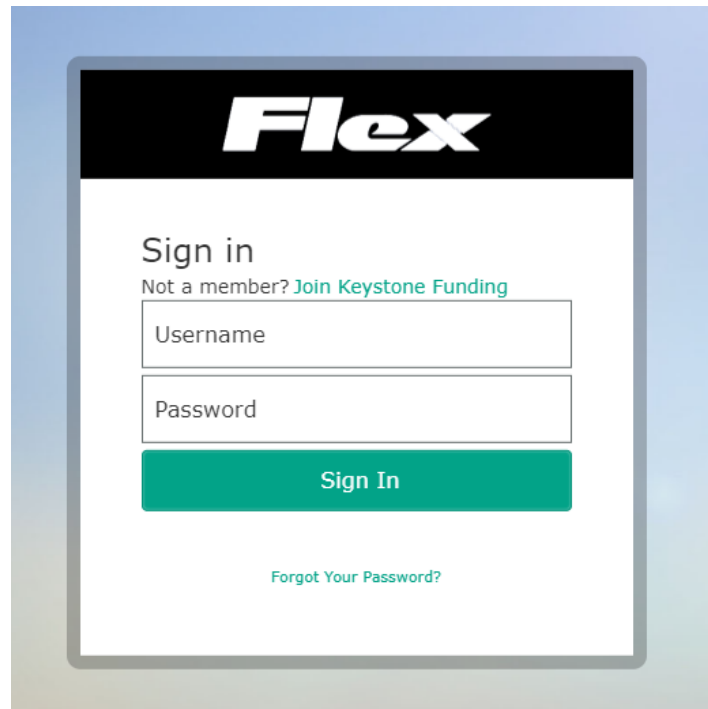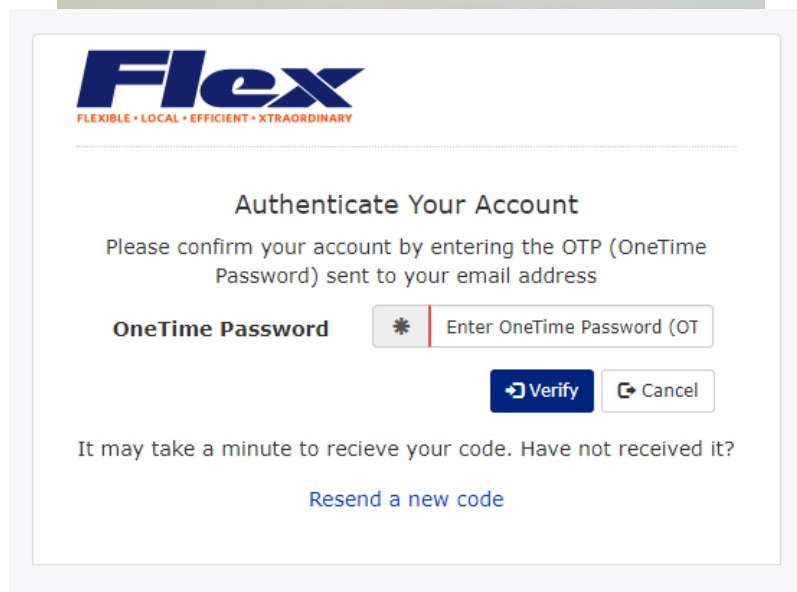
The below guidance details the instructions for logging into FLEX using either the **Email** or **Device** option, how to update your authentication preference, as well as how to download authenticators for the Device option.

If you have any questions, please contact your Account Executive.

Accessing FLEX via Multi Factor Authentication (MFA)

**The below steps will be repeated during each login session with FLEX.**

1. Navigate to FLEX
2. Enter your assigned Username and Password and select the "Sign In" button.
   a. If you need a Username and Password, please reach out to your Account Executive to have this set up.
3. After entering your credentials, you will reach the MFA page requesting the one-time passcode.

EMAIL OPTION

If your account is set up to receive an emailed one-time passcode, the passcode will automatically be sent to the assigned email address in your user profile during the log in process.

1. The email will come from noreply@fibiz.fiserv.com. Please check your spam or junk folder if you do not receive it in your inbox.
   a. The Subject Line will read as: Mortgage Director - OTP
2. Within the body of the email, there will be a 6-digit code provided. Enter this code on the FLEX MFA Screen to verify your entry.
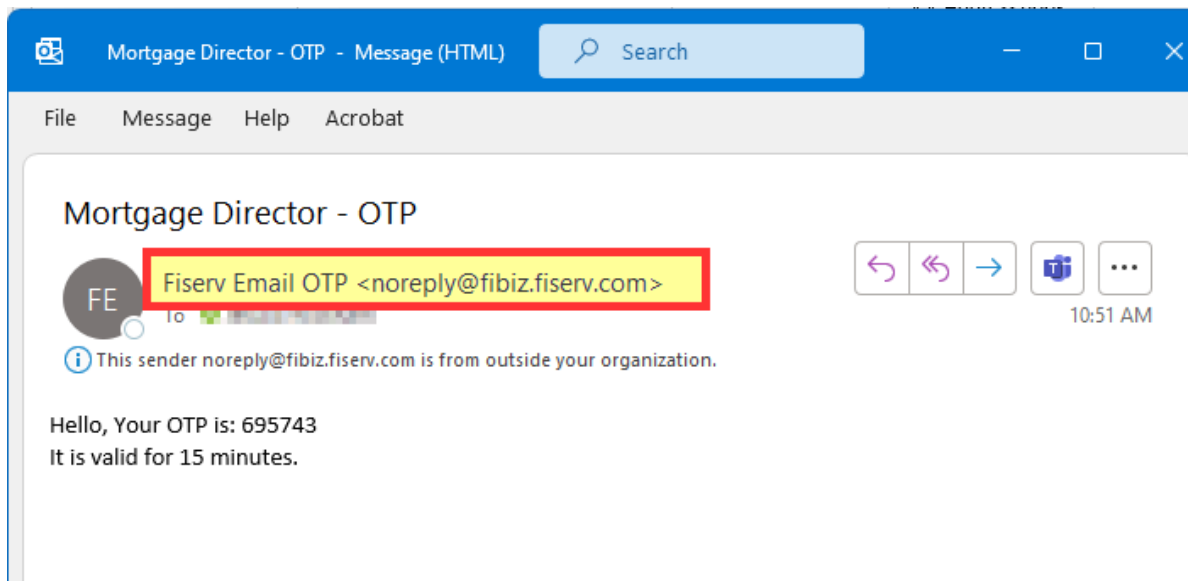
DEVICE OPTION

If your account is set up to receive a one-time passcode via a third-party authenticator app, you will need to open the app (in either your browser or phone) to access the given code. Enter the code to verify your entry.
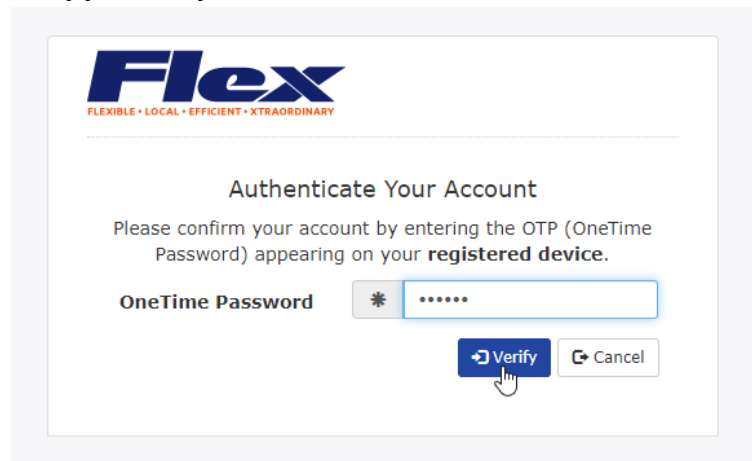
While a variety of authenticator applications work with the FLEX Portal, not all are supported. The following are confirmed supported with FLEX at this time.

Mobile Apps:

- Twilio Authy
- Authly
- Google Authenticator
- Microsoft Authenticator

Computer Options:

- Chrome Extension - Google Authenticator https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai
- Microsoft Edge Add On - https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknglpdipeoio

Please reference the guidance below for downloading a 3rd party authenticator via a web browser or phone app.

Updating your Authentication Preferences in FLEX

Overview: Multi Factor Authentication is required to access Keystone Funding's FLEX portal. There are two available options to receive a one-time passcode, Email and Device. If the Device option is preferred, it must be manually selected within the user's profile and the following steps must be followed to link their FLEX account with a third-party authenticator.
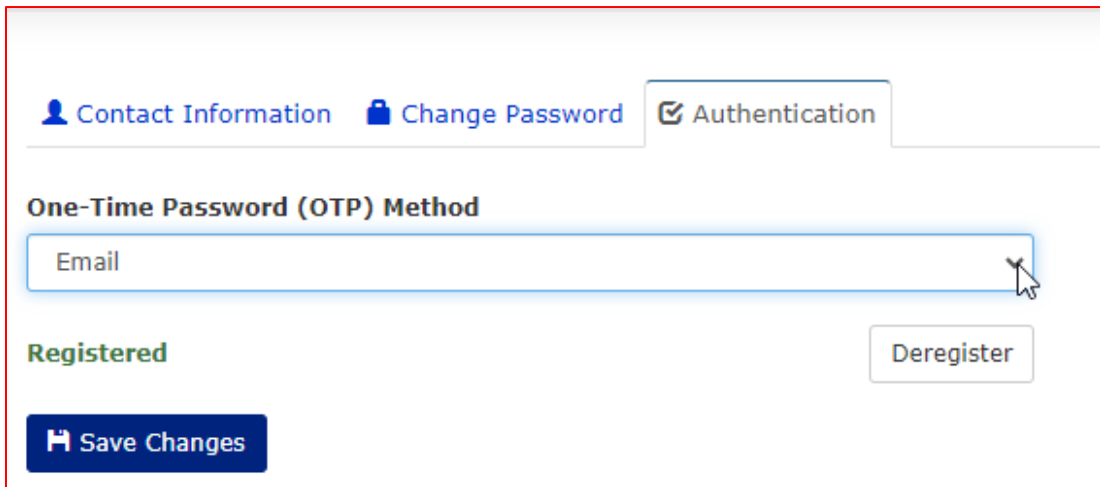
1. Upon successfully logging into FLEX, navigate to the new SETTINGS menu option:
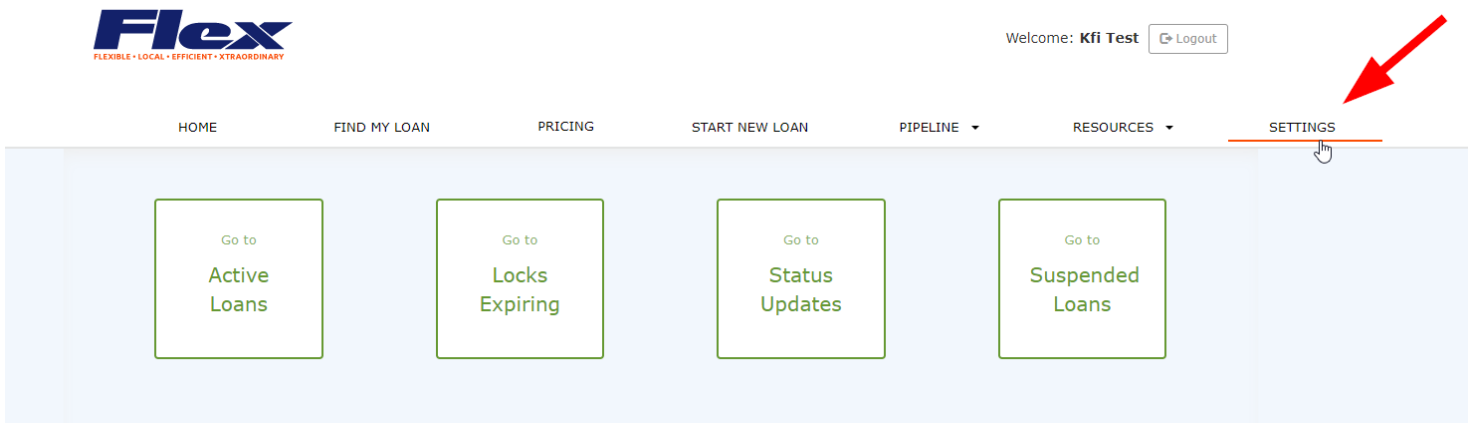
2. Here you can review your profile settings, change your password, and update your authentication preferences.
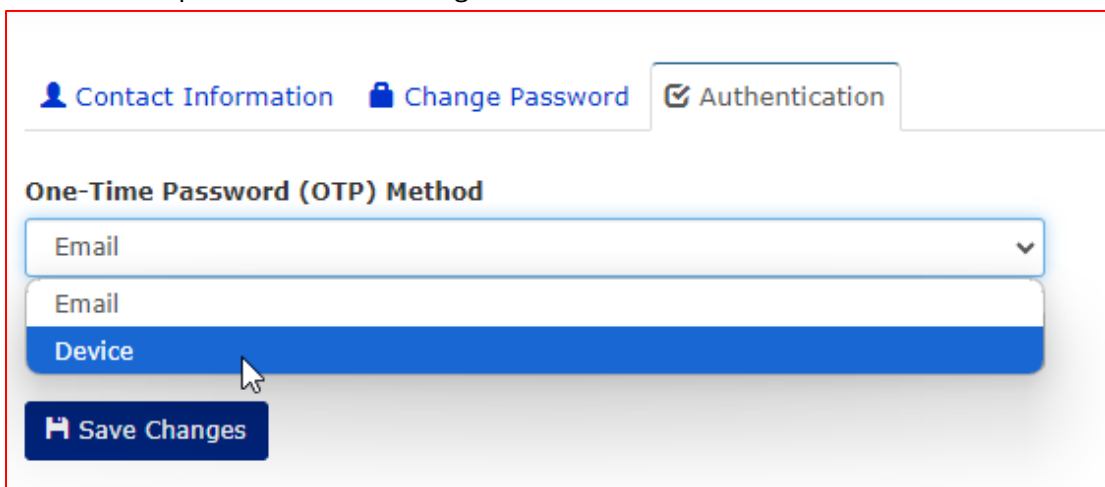3. Select the Authentication tab
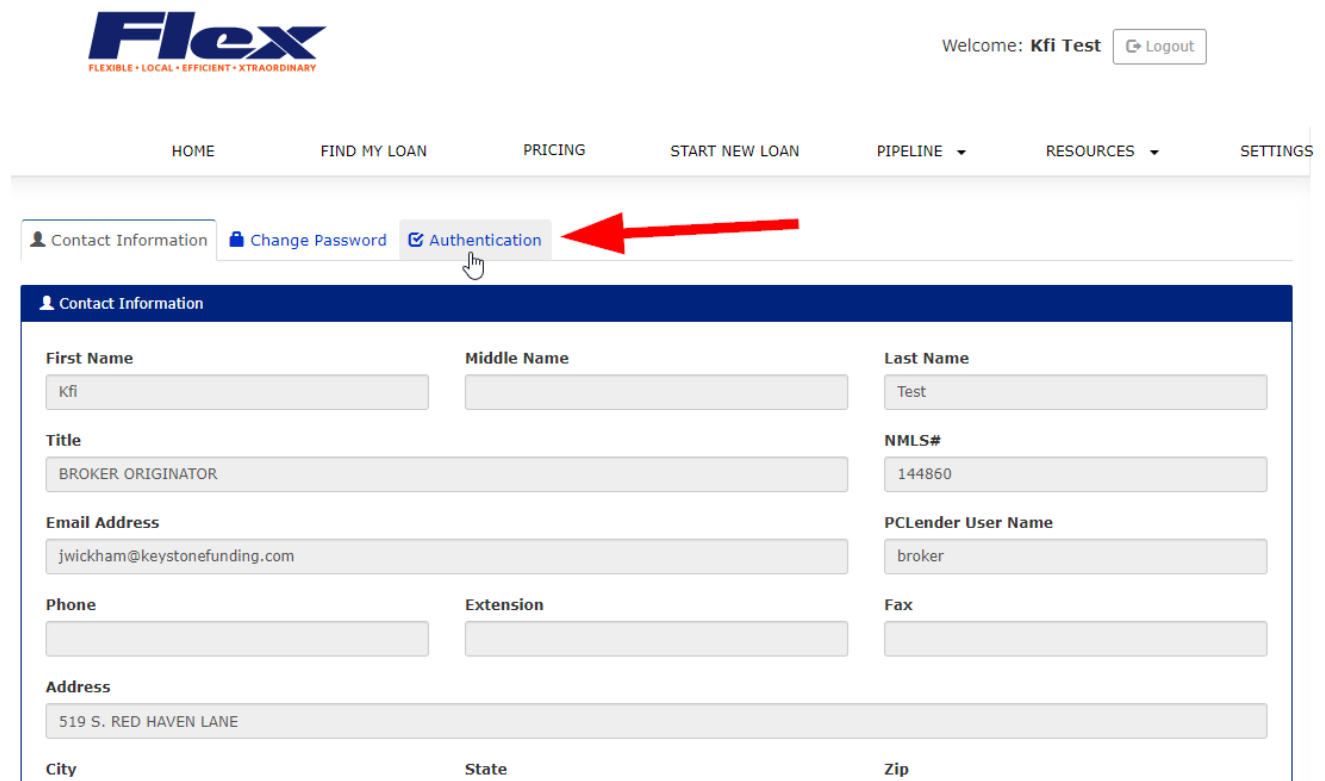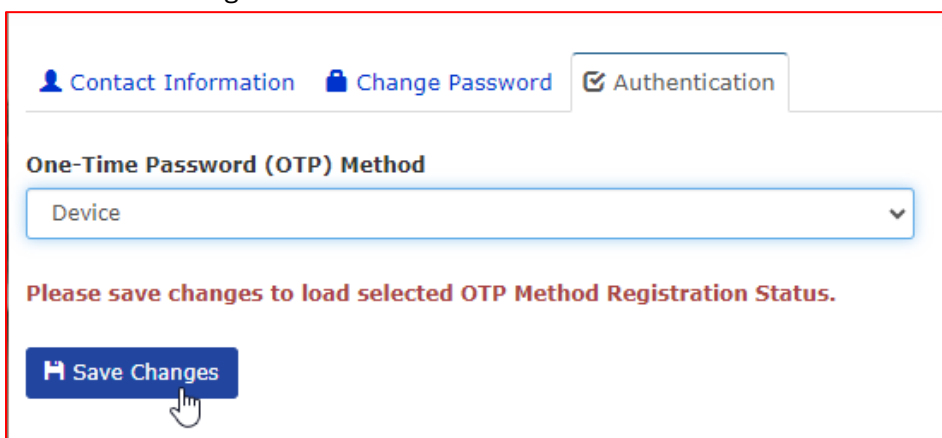
***By default, the EMAIL option will be selected.

4. Select the drop-down arrow to change the selection from Email to Device

5. Select Save Changes
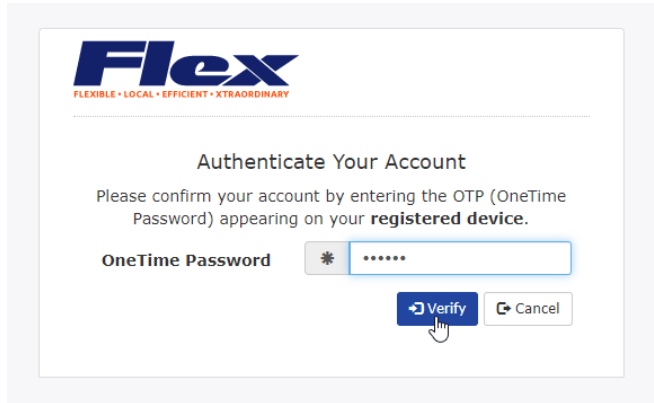
6. Review the confirmation window stating that the setting has been updated, Close the window.

Authentication Settings Changed

Authentication Settings have successfully updated.

Close
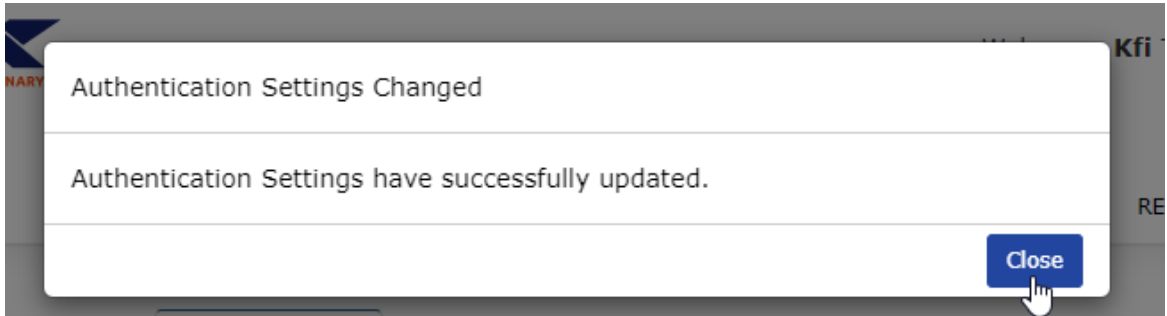
7. On your next login, you will be prompted to register your account with a third-party authenticator before accessing FLEX.

Sign in

Not a member? Join Keystone Funding

broker

••••••••••

Sign In

Forgot Your Password?

Complete the following steps to configure your authenticator app:

1. Install your authenticator app of choice to your phone or computer.

2. In the app, add an account. Follow the prompts until a code is required.

3. Scan the image below:

If you are unable to scan the image, enter the following code in your app:

PLSUMD6VIDY3G4EVAT25H64R7VF7WLYS

If your app displays a six-digit code, congratulations, your device is registered! Click next to continue logging in.

Next   Cancel

8. Following Registration with a Third-Party Authenticator (instructions below), the next screen presented will be where to enter the provided authentication code.

9. Enter the code and select Verify to enter FLEX:

You will be prompted to enter a One Time Passcode with each login session to Flex.

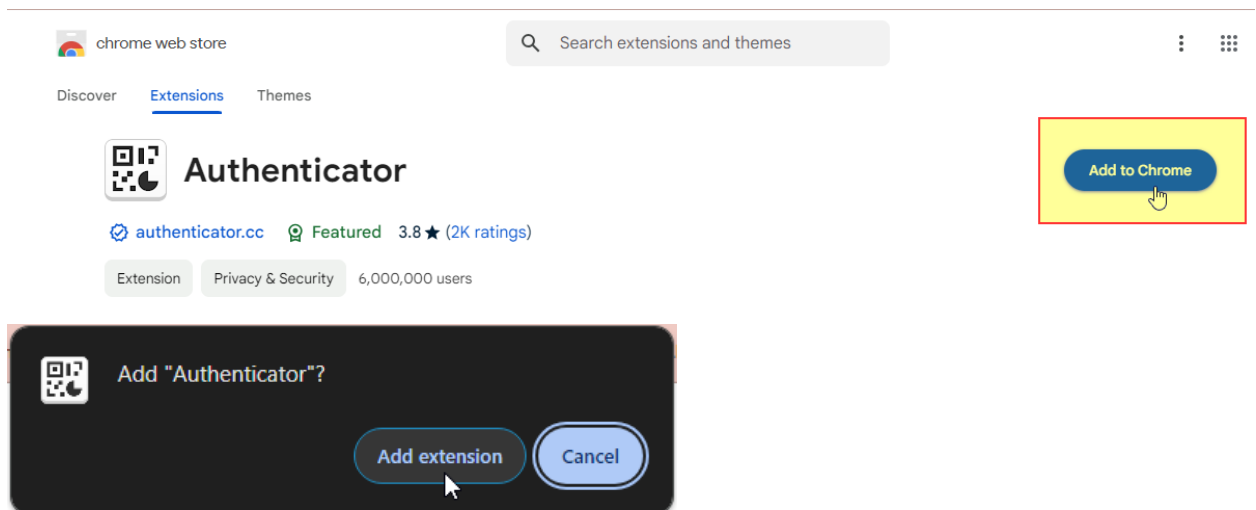# Web Browser Authenticator (Google Authenticator)

Overview: Multi Factor Authentication is required to access Keystone Funding's FLEX portal. There are two available options to receive a one-time passcode, Email and Device. If the Device option is selected in your user profile, a web browser authenticator such as Google Authenticator is one way to receive the one-time passcode.

The instructions listed in this guide are for downloading Google Authenticator and linking your FLEX account; however, other browser-based authenticators or phone based apps are acceptable.
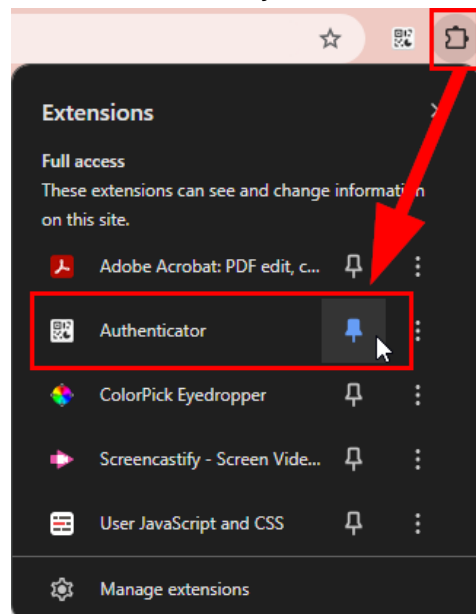
Google Authenticator can be found at:

https://chromewebstore.google.com/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai?hl=en

1. Select the "Add to Chrome" button > Add the Extension


2. Pin the extension to your browser toolbar

3. Return to the FLEX login screen where the QR code is presented.
    a. Select the newly pinned Authenticator Icon (at the top, right of the URL)
    b. Select the QR code icon (highlighted in snippet) to scan the QR code
        i. Use your mouse to click and drag a box around the QR code on the FLEX screen– the Google Authenticator should recognize it and link it automatically.
4. Select NEXT when finished
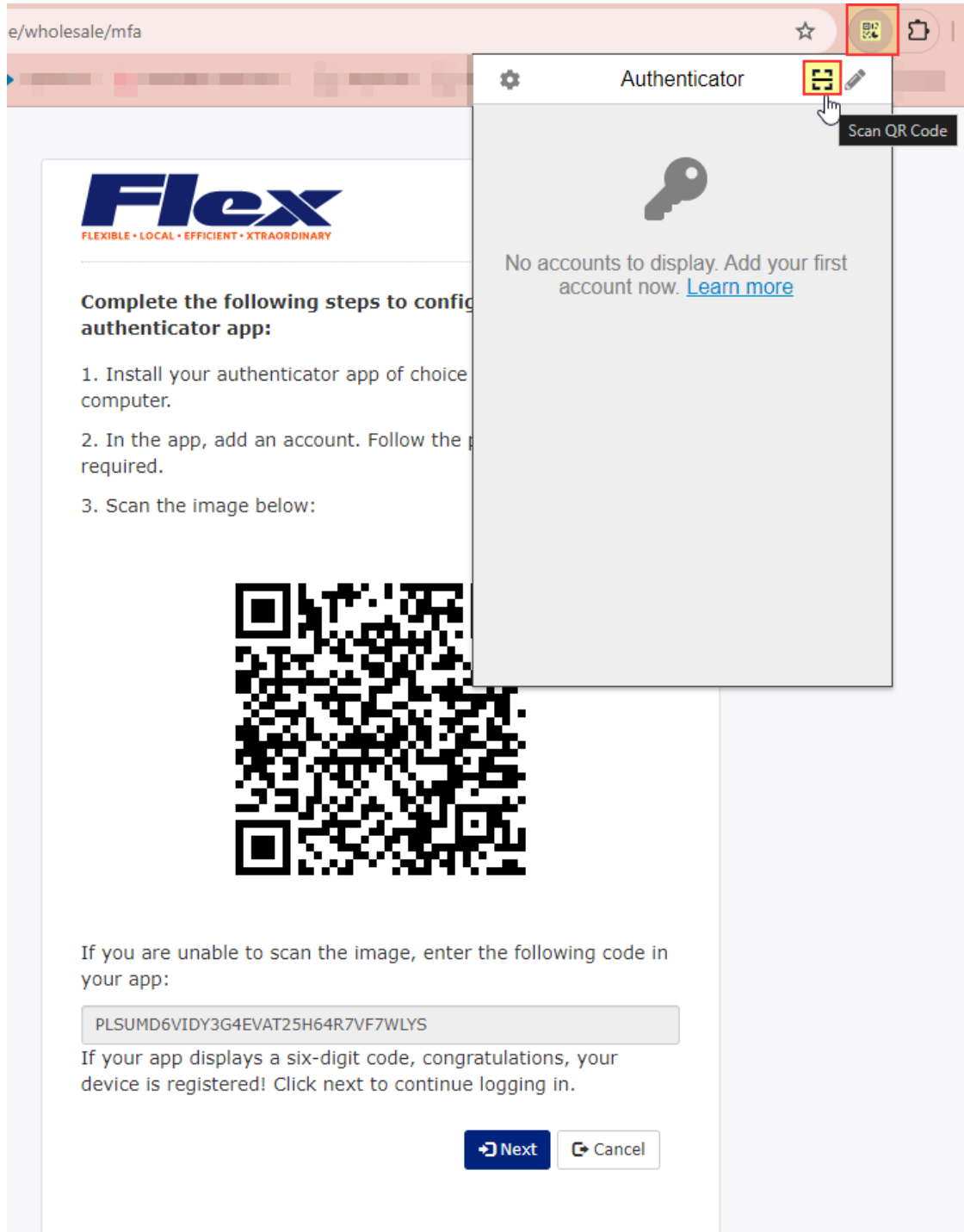
5. You'll be directed to a new screen to enter the authentication code.
6. Select the Authenticator Icon as before (next to the URL)
   a. This time a One Time Passcode will be displayed.
7. Select the provided code to copy it
8. Paste the code into the OneTime Password field for FLEX
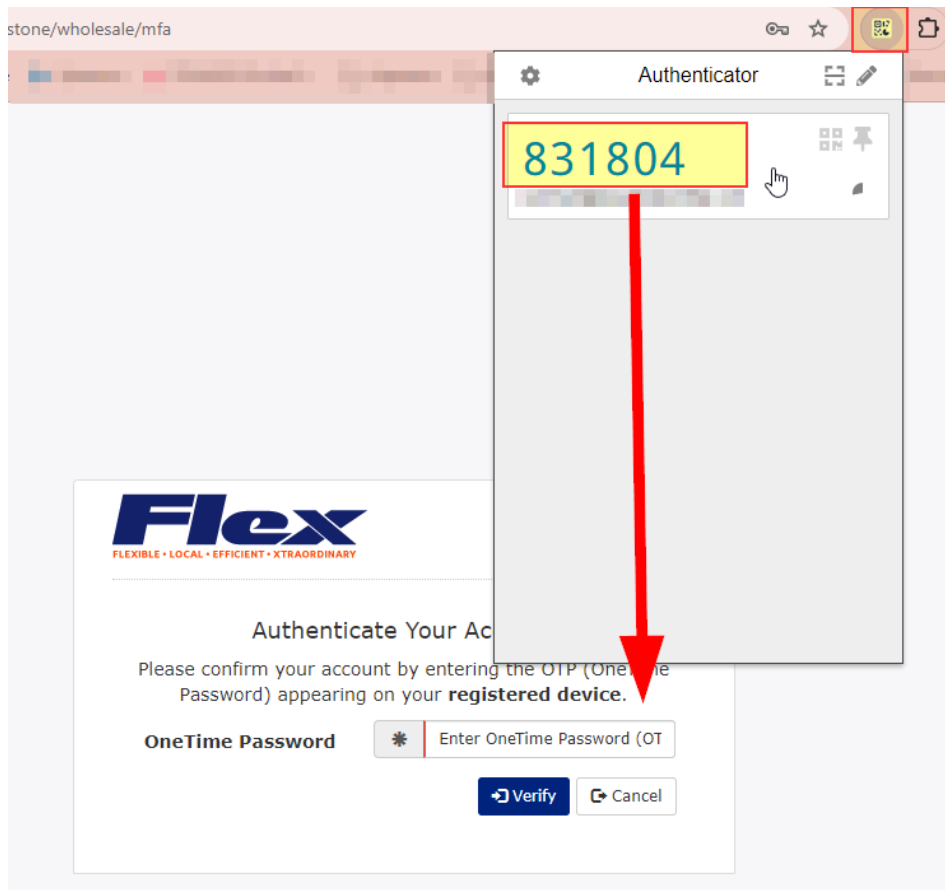
9. Select Verify to enter FLEX:
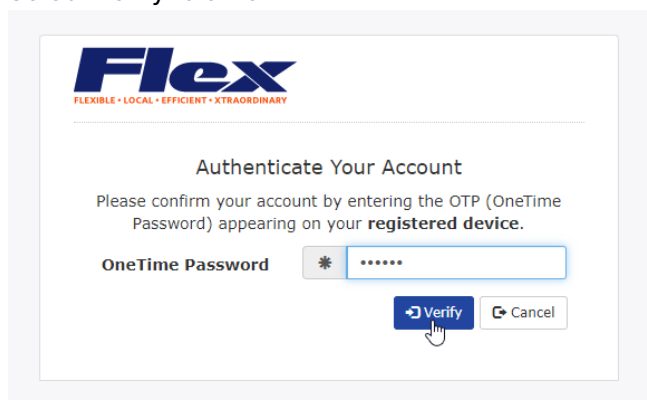
You will only need to **register** your device once; but you will be required to enter a OneTime Password with each login.

Phone App Authenticator (Twilio Authy)

Overview: Multi Factor Authentication is required to access Keystone Funding's FLEX portal. There are two available options to receive a one-time passcode, Email and Device. If the Device option is selected in your user profile, an app authenticator on your hand held device such as Twilio Authy is one way to receive the one-time passcode.

The instructions listed in this guide are for downloading Twilio Authy and linking your FLEX account; however, other browser-based authenticators or phone-based apps are acceptable, such as:

- Authly
- Google Authenticator
- Microsoft Authenticator

1. **Access the App Store or Google Play on your device**.
2. Search for Twilio Authy, download the app
3. Twilio Authy will prompt you to create an account before proceeding further
    a. Follow the steps to create your account.
4. After you've created your account, the app will present a page where you have the option to add new accounts.
In the following example, you will click the **+** sign when ready to register a new account for FLEX.

![Keystone Funding logo]
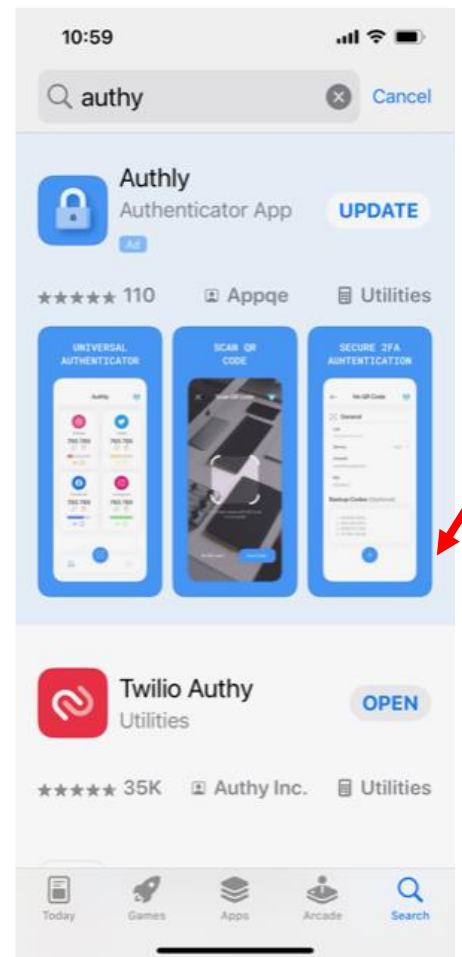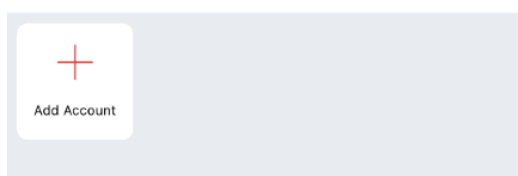
5. When you click the **+** option, the App presents an option to scan a QR code **OR** enter the key manually.

Cancel   **Add Account**

Scan the QR Code on the website where you are enabling 2FA.
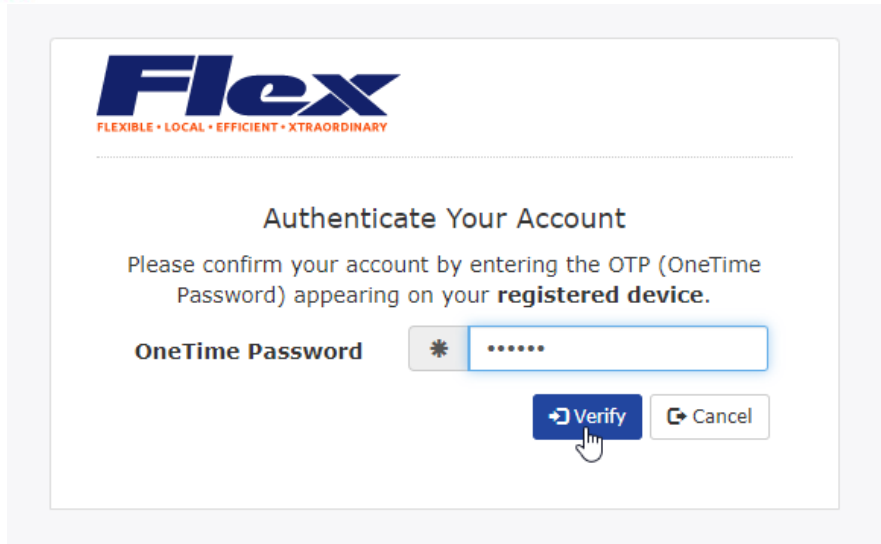
[📷] Scan QR Code

No QR code? Enter key manually.

    a. Return to the FLEX login screen where the QR code is presented.

    b. Use the "Scan QR Code" button to scan the QR code on the FLEX screen OR select the "Enter key manually" link to enter the code manually as needed:
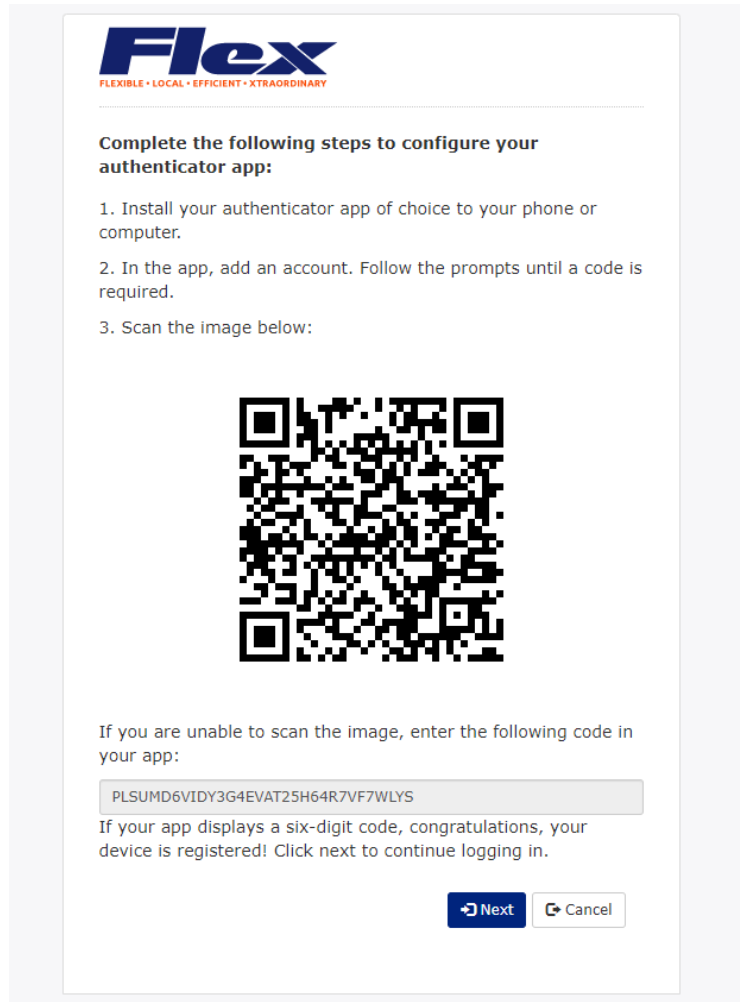
6. Select NEXT on the FLEX window when finished.
    a. You'll be directed to a new screen to enter the authentication code.
7. After you've successfully connected FLEX to Twilio Authy, the app displays the 6-digit code for entering FLEX.
8. Enter the code and select VERIFY on the FLEX window to proceed into the portal.

You will only need to **register** your device once; but you will be required to enter a OneTime Password with each login.