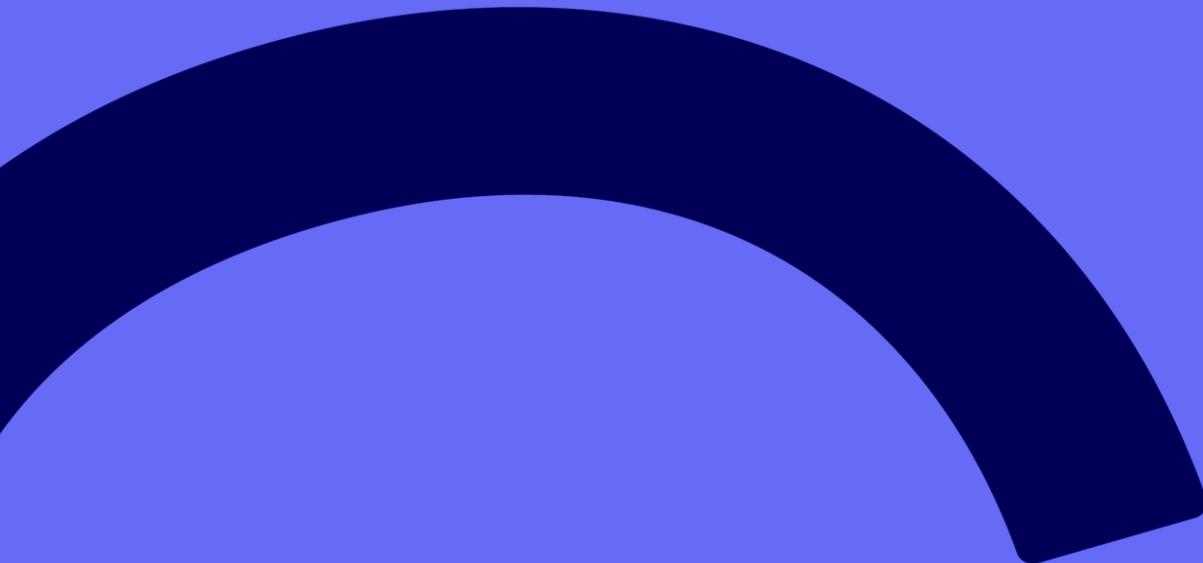


A thick, dark blue curved graphic element, resembling a stylized arch or a partial circle, located in the top left corner of the slide.

Multi-factor Authentication (MFA) Setup Guide

Multi-factor Authentication (MFA)

Multi-factor authentication (MFA) is a way to further secure access to sensitive data by requiring an additional verification method to access an account. Even if a user's password is compromised, the bad actor will still be unable to access the account without access to the additional verification method.

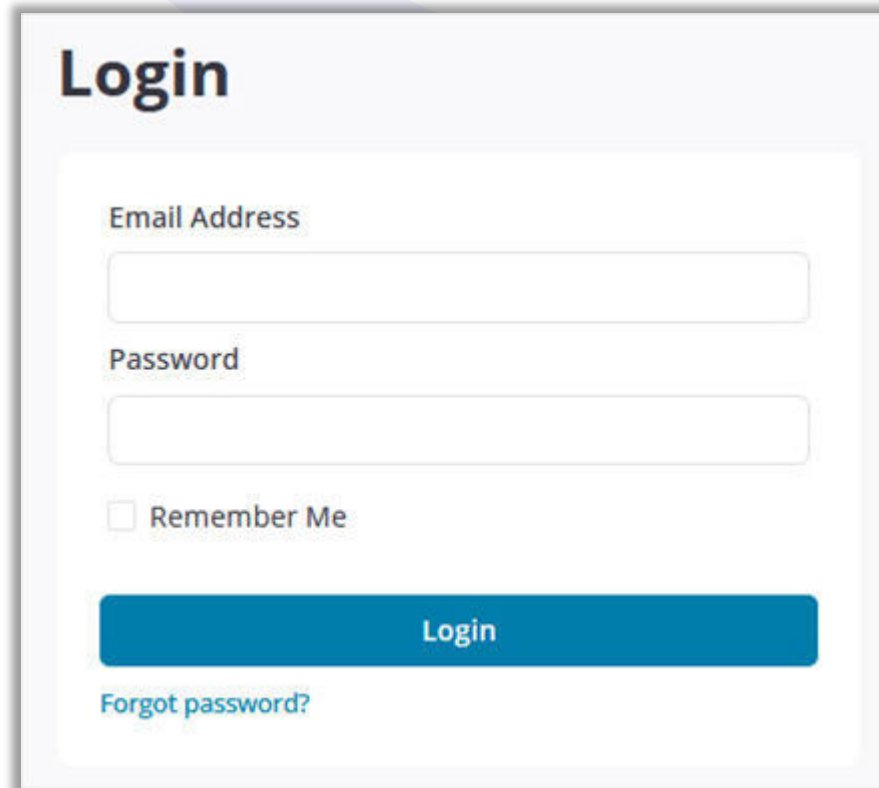
In mid-2026, Pennie transitioned from Duo to Keycloak as the MFA provider. Keycloak utilizes time-out one-time passcode (TOTP) for verification. TOTP is an MFA method where a registered app or device generates a 6-digit code that changes every 30 seconds. After entering their username and password, the user must enter the current code to complete login.

Users may use any standard TOTP-compatible application, including:

- Google Authenticator
- Microsoft Authenticator
- Duo (in OTP mode)
- FreeOTP
- Apple Password Manager
- Other standard TOTP-compatible apps
- Browser-based authenticator extensions may also work, such as Authenticator.cc for Chrome, Edge, and Firefox

MFA First-time Setup: Mobile App Option

1. To set up your new MFA method, log in with your username and password as you would normally:

A login form with a light gray border and a white background. At the top left, the word "Login" is written in a bold, dark gray font. Below it, the label "Email Address" is positioned above a white rectangular input field. Further down, the label "Password" is above another white rectangular input field. Below the password field, there is a checkbox followed by the text "Remember Me". At the bottom of the form, there is a solid blue rectangular button with the word "Login" in white text. Below the button, the text "Forgot password?" is displayed in a smaller, blue font.

Login

Email Address

Password

☐ Remember Me

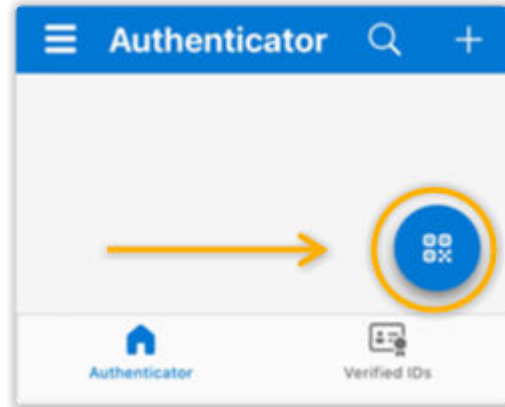
Login

[Forgot password?](#)

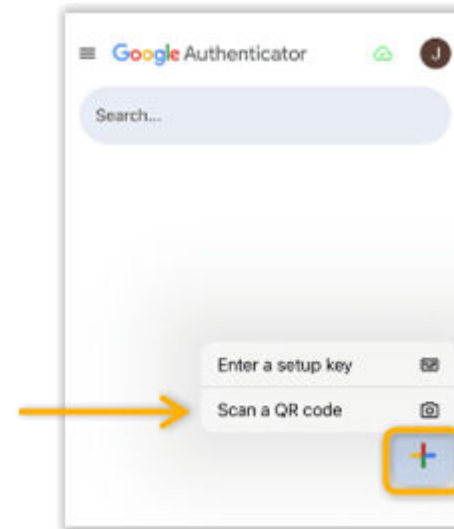
You will be prompted to set up multi-factor authentication. Select the **Use an authenticator mobile app** option.

MFA First-time Setup: Mobile App Option

2. If you don't have one already, you will need to download a mobile authentication program from your phone's app store.
3. Once downloaded, open the app. *In the app*, select **Scan QR Code**.
 - This should automatically open your phone's camera.
 - Depending on the app, this may be a button with a QR code icon, an option titled "Add Account," or something similar.



(Microsoft Authenticator)

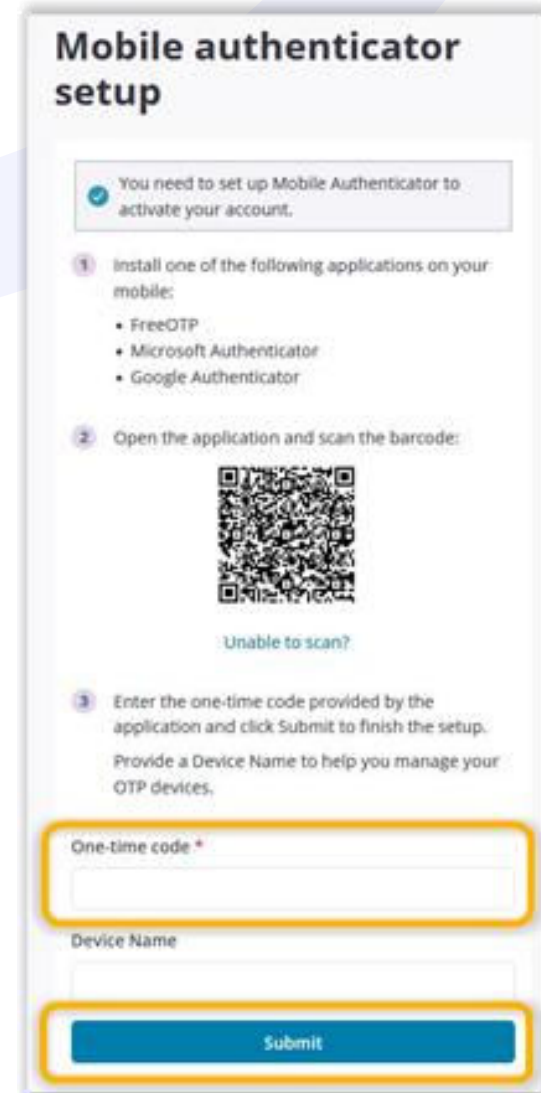


(Google Authenticator)

MFA First-time Setup: Mobile App Option

4. Once the camera has opened, scan the QR code *on the computer screen* with your camera.
 - A new account will be added to your authenticator app and immediately begin providing 6-digit codes.
5. Enter the code shown into the **One-time code** field on the setup screen, then click **Submit**.

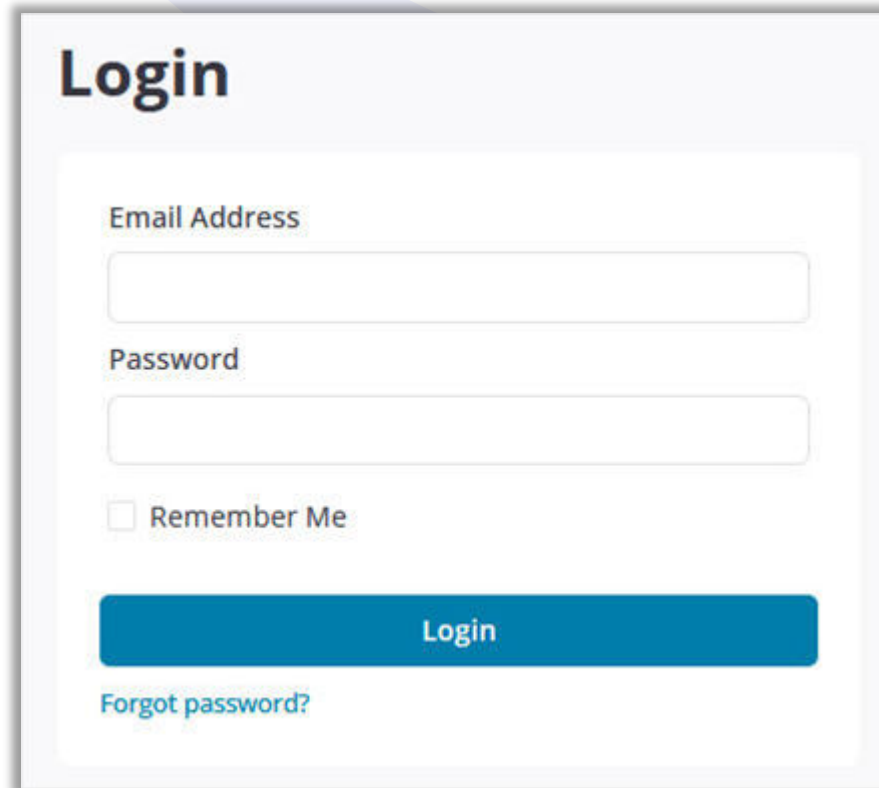
Note: There is a timeout of 5 minutes once you get to Step 3. If you don't complete Step 5 in that time, you will be asked to login again.



The screenshot shows a 'Mobile authenticator setup' interface. At the top, a message states: 'You need to set up Mobile Authenticator to activate your account.' Below this, there are three numbered steps: 1. 'Install one of the following applications on your mobile:' with a list of 'FreeOTP', 'Microsoft Authenticator', and 'Google Authenticator'. 2. 'Open the application and scan the barcode:' which includes a QR code and a link 'Unable to scan?'. 3. 'Enter the one-time code provided by the application and click Submit to finish the setup.' This step also prompts the user to 'Provide a Device Name to help you manage your OTP devices.' At the bottom, there are two input fields: 'One-time code *' and 'Device Name'. A blue 'Submit' button is located at the very bottom of the form.

MFA First-time Setup: Browser Extension Option

If you are unable to use a mobile phone for authentication, you can opt to use a web browser extension.

A login form with a light gray border and a white background. At the top left is the title "Login" in bold black text. Below it are two input fields: "Email Address" and "Password", both with light gray borders. Below the password field is a checkbox labeled "Remember Me". At the bottom is a blue button with the text "Login" in white. Below the button is a link that says "Forgot password?" in blue text.

Login

Email Address

Password

☐ Remember Me

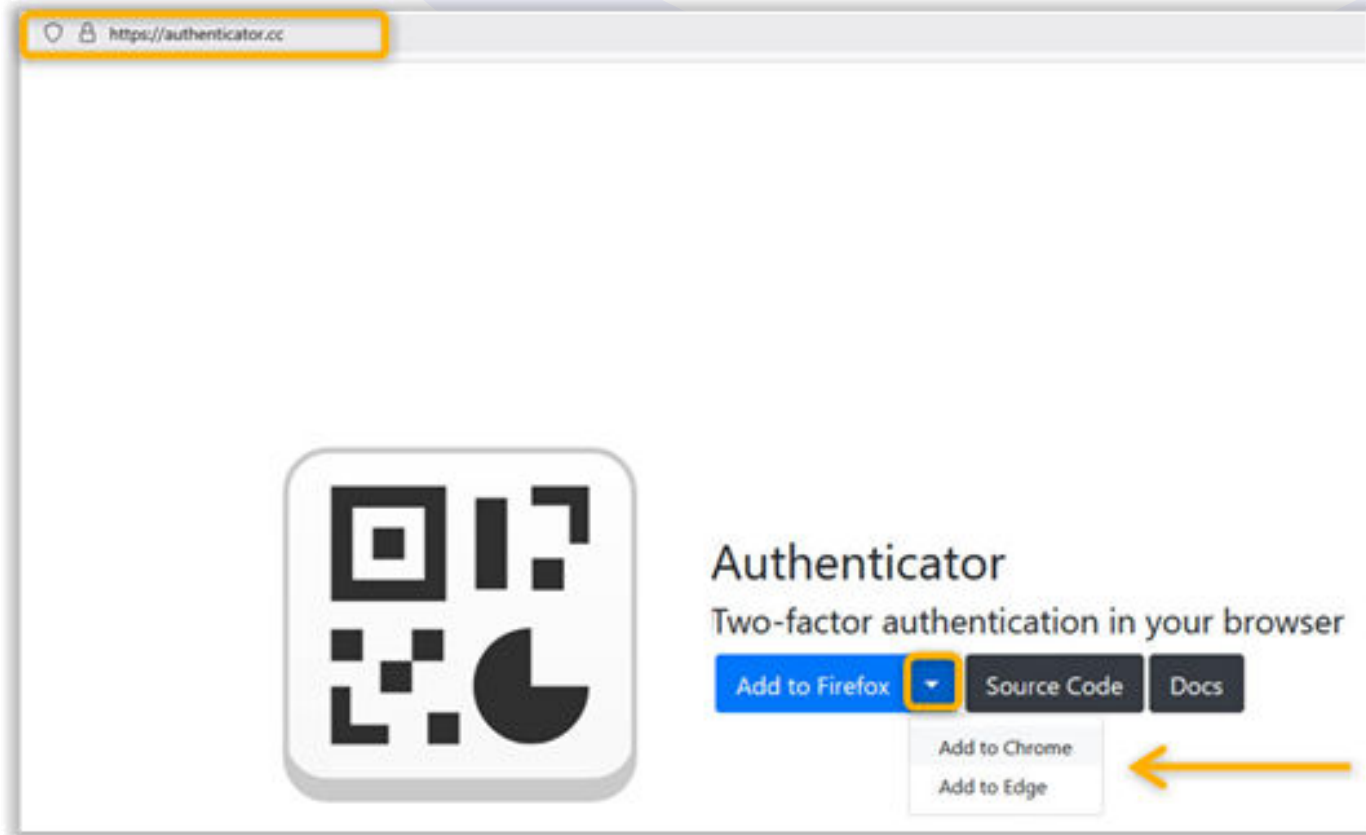
Login

[Forgot password?](#)

1. As with the mobile app option, log in with your username and password, then select the **Use an authenticator mobile app** option.

MFA First-time Setup: Browser Extension Option

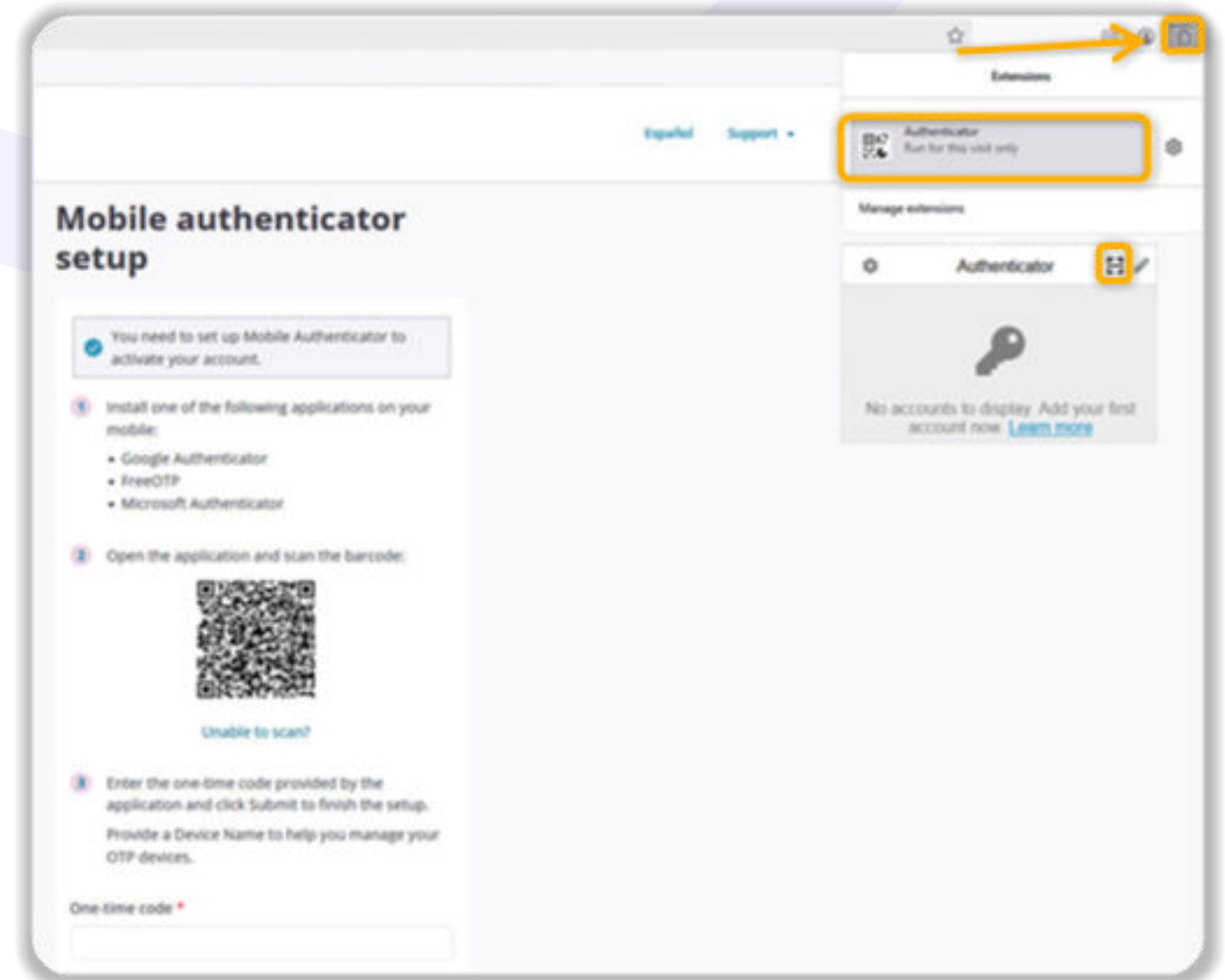
2. With the TOTP setup screen up, open a new browser tab and go to **authenticator.cc**.



Select the option that corresponds with your browser.

MFA First-time Setup: Browser Extension Option

3. Return to the **Mobile authenticator setup** tab.
4. Open the newly-downloaded browser extension by clicking on the puzzle icon, then the QR scan icon.
 - This will activate the QR code scanning feature within your browser.



MFA First-time Setup: Browser Extension Option

- From here, click and drag your mouse cursor over the entire QR code on the **Mobile authenticator setup** screen.



The screenshot shows the 'Mobile authenticator setup' interface. It includes a message: 'You need to set up Mobile Authenticator to activate your account.' Below this, step 1 lists applications to install: Google Authenticator, FreeOTP, and Microsoft Authenticator. Step 2 shows a QR code with a red dashed box around it and a red callout bubble saying 'Drag cursor to cover entire QR code.' Below the QR code is a link 'Unable to scan?'. Step 3 instructs the user to enter a one-time code and provide a device name. At the bottom are input fields for 'One-time code *' and 'Device Name'.

Mobile authenticator setup

You need to set up Mobile Authenticator to activate your account.

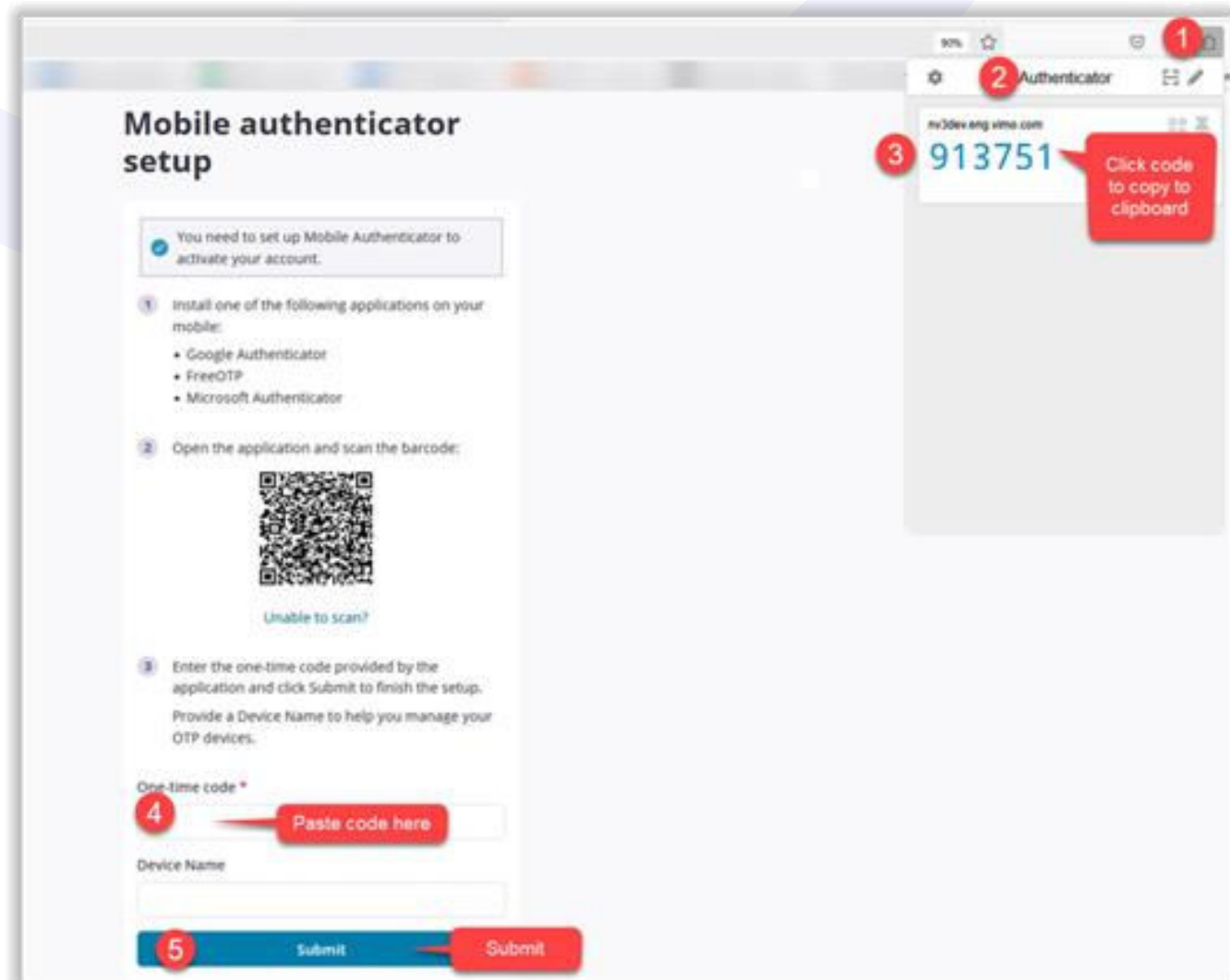
1. Install one of the following applications on your mobile:
 - Google Authenticator
 - FreeOTP
 - Microsoft Authenticator
2. Open the application and scan the QR code:
[Unable to scan?](#)
3. Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.

One-time code *

Device Name

MFA First-time Setup: Browser Extension Option

6. If scanned successfully, you'll see a confirmation screen that the username has been successfully added. Click "OK" to close window.
7. Reopen the browser extension by clicking on the puzzle icon. You should now see a 6-digit TOTP code.
 - Click on the code to copy it to your clipboard.
8. Click on the **One-time code** box and paste the code.
9. Click **Submit**.



pennie[®]

ADDRESS

P.O. Box 11873

Harrisburg, PA 17108-1873

PHONE

+1 844-844-8040

WEB

pennie.com