



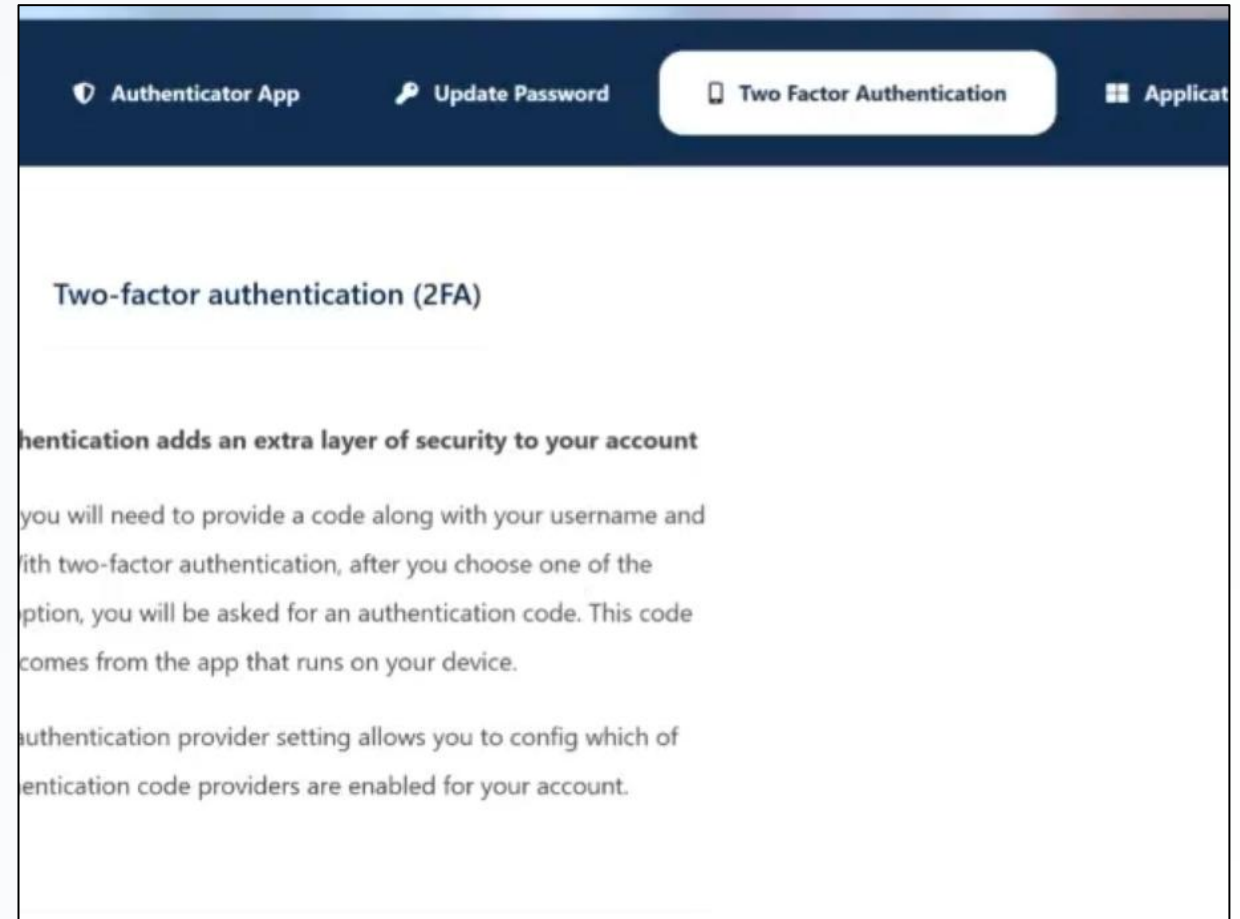
# **Two-Factor Authentication (2FA)**

# 1. Check 2FA Tab

## Verify @ Factor Availability

Log into your account dashboard to check if Multi-Factor Authentication configuration is authorized for your account profile.




-  Look at the main navigation bar.
-  Click on the **Two factor authentication** tab.

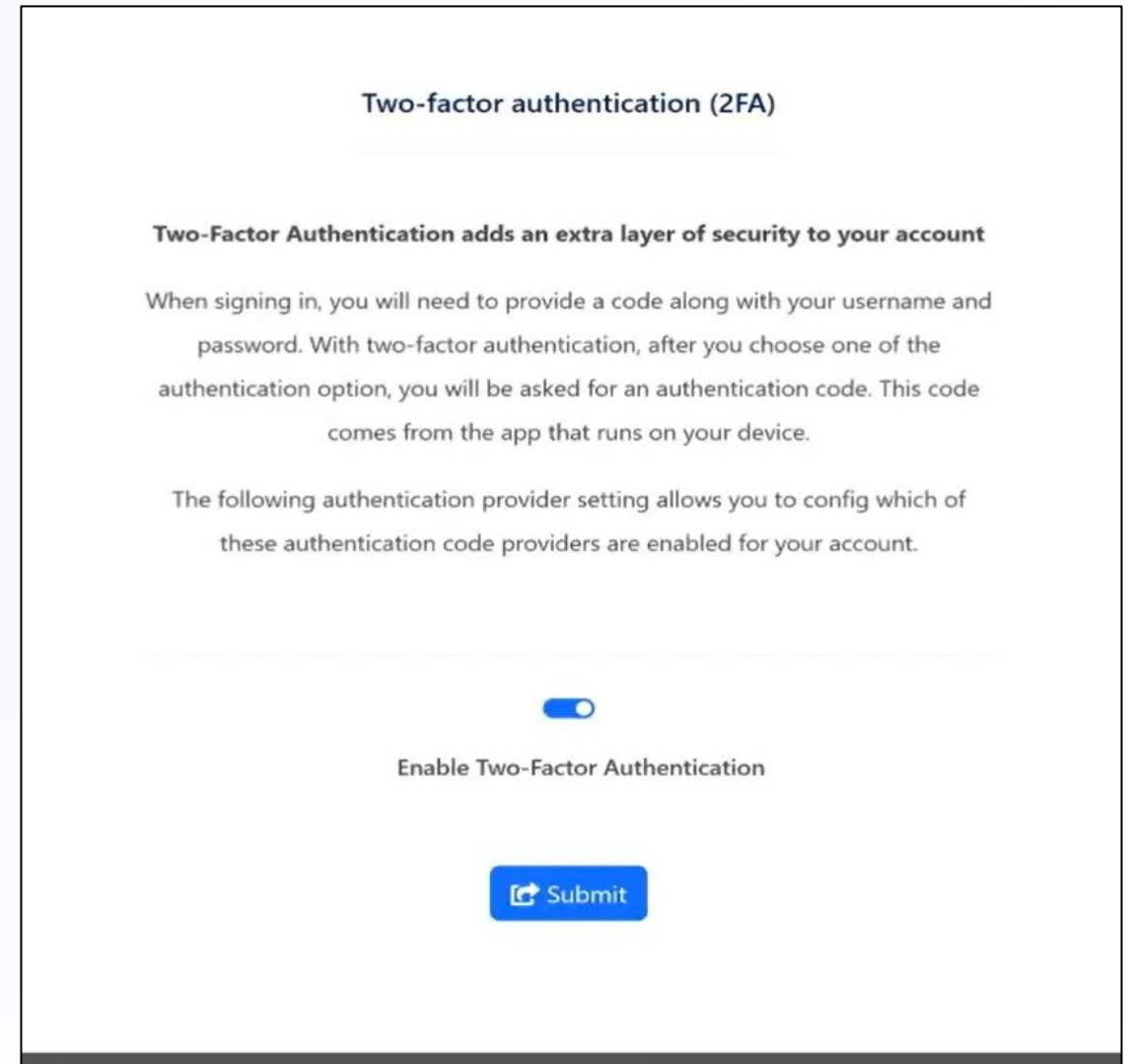


# | 2. Enable & Submit

## Activate Security Lock

If you see the settings panel controls, you are ready to apply the multi-layer security configuration.

-  Ensure the toggle switch is turned to **Enabled**.
-  Press the **Submit** button to commit the activation.
-  *Missing the controls?* You must contact a GPO Admin to enable MFA modifications for your account.



# Supported Verification Channels

GPO IMS supports multiple secure mechanisms for receiving your temporary verification security codes:



## E-mail

Delivered securely to your registered organizational inbox profile.



## Phone SMS

Sent via text message. Requires verification inside the *Add Phone Number* tab.






## Authenticator App

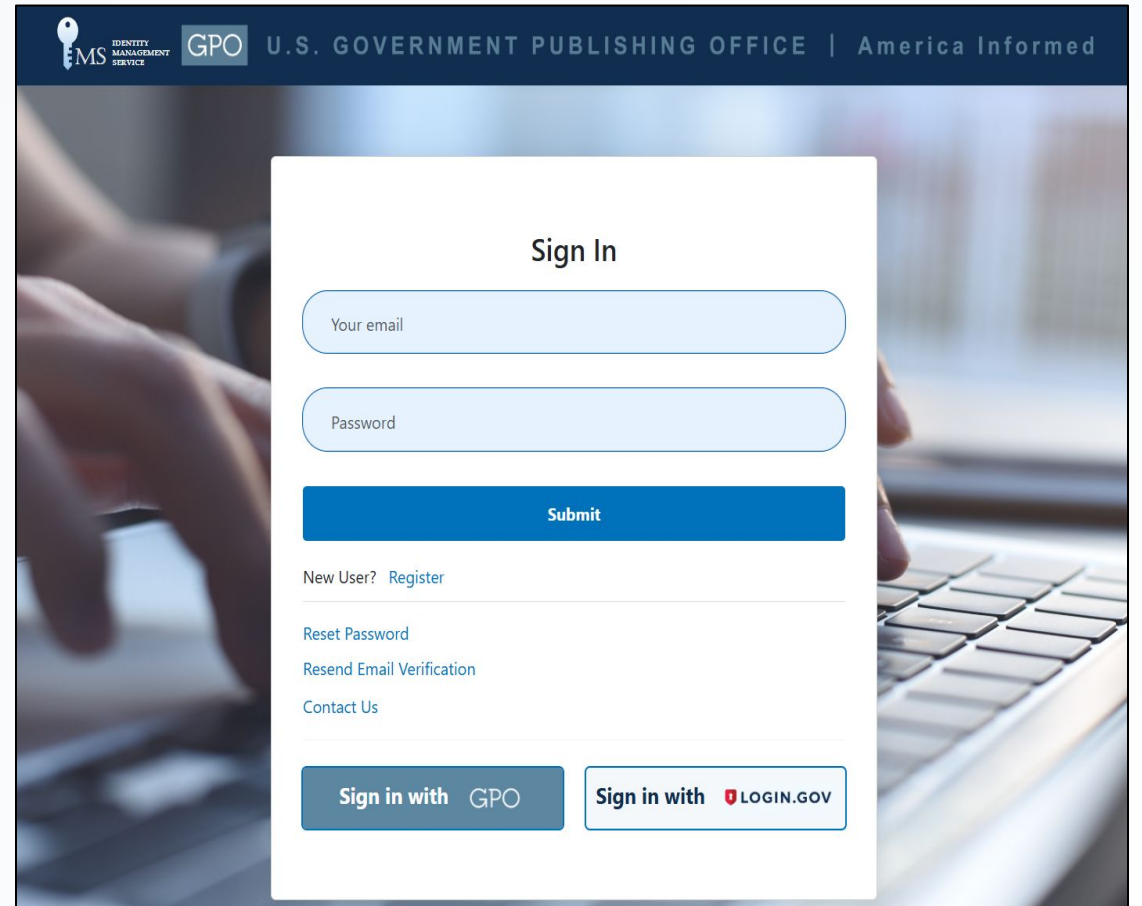
Generates real-time localized codes via standardized authenticator apps.

# 3. Regular Initial Entry

## Standard Authentication Step

When logging into an account with active protection, start by entering your credentials exactly as normal.

-  Input your associated registered Email.
-  Input your account Password.
-  Click the standard login button to continue.



The screenshot shows the 'Sign In' page for the U.S. Government Publishing Office (GPO). The page features a dark blue header with the GPO logo and the text 'U.S. GOVERNMENT PUBLISHING OFFICE | America Informed'. The main content area is white and contains a 'Sign In' form. The form has two input fields: 'Your email' and 'Password'. Below the input fields is a blue 'Submit' button. Underneath the 'Submit' button are links for 'New User? Register', 'Reset Password', 'Resend Email Verification', and 'Contact Us'. At the bottom of the form are two buttons: 'Sign in with GPO' and 'Sign in with LOGIN.GOV'.

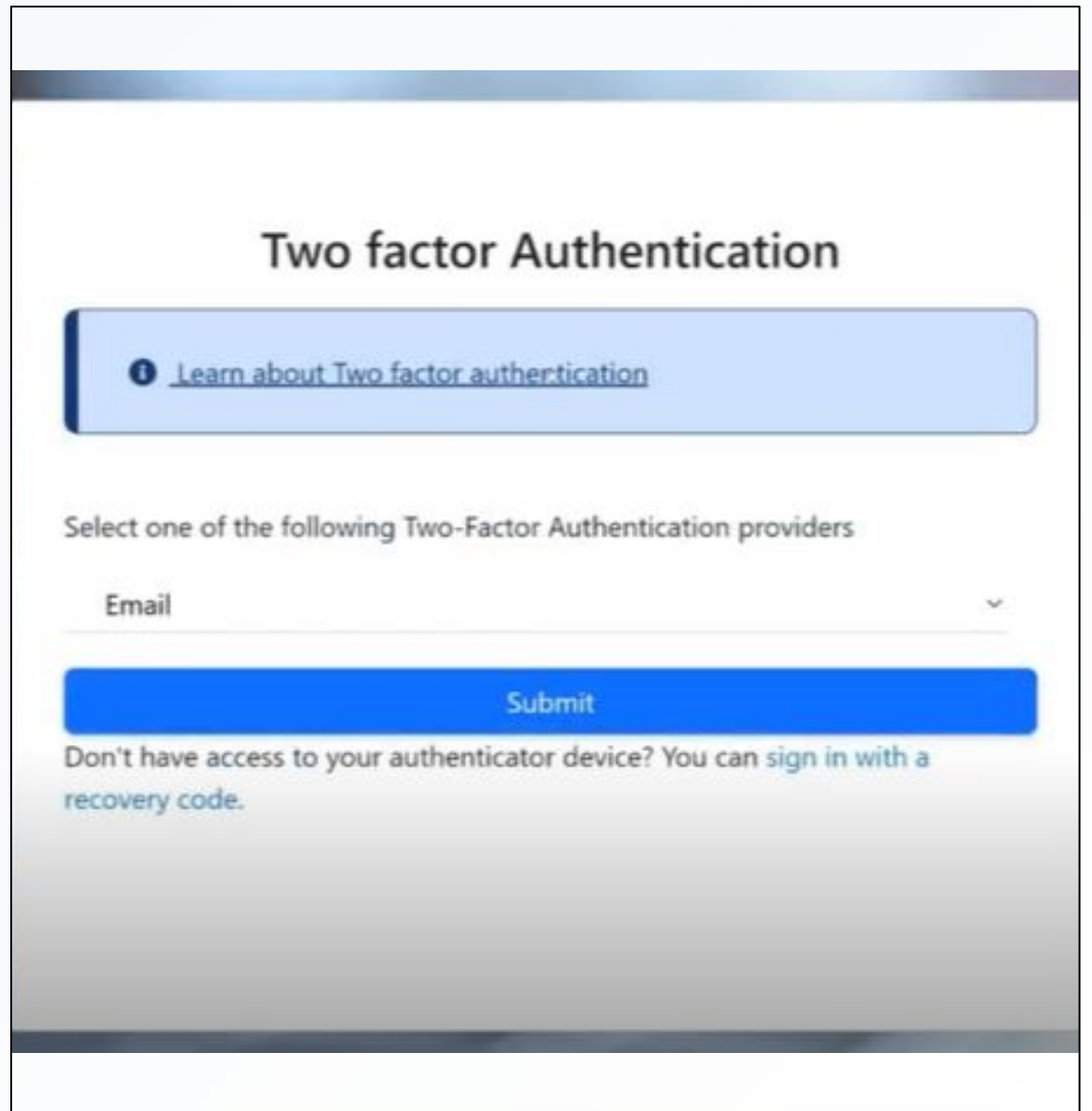
# 4. Select Delivery Method

## Choose Secondary Layer

After initial step verification, the system safely redirects you to a protection challenge screen.

 Select your preferred method to receive the dynamic token.

 Note: It may take 1 to 2 minutes for the transmission to arrive.



The screenshot shows a mobile application interface for Two factor Authentication. At the top, the title "Two factor Authentication" is centered. Below the title is a light blue rounded rectangle containing an information icon and a link: "Learn about Two factor authentication". Underneath this is the instruction "Select one of the following Two-Factor Authentication providers". A dropdown menu is open, showing "Email" as the selected option. Below the dropdown is a prominent blue "Submit" button. At the bottom of the screen, there is a note: "Don't have access to your authenticator device? You can sign in with a recovery code."

# 5. Enter Verification Code

## Input Temporary Token

Retrieve the security token from your chosen device channel and return to the portal window to finalise identity confirmation.



Type the secure code into the input field carefully.



Submit the code to open your dashboard account workspace safely.

The screenshot shows a web form titled "Two factor Authentication". At the top, there is a light blue button with an information icon and the text "Learn about Two factor authentication". Below this is the instruction "Please enter the authentication code below". A large, light blue input field is labeled "Sign-in code". Underneath the input field is a blue "Submit" button. At the bottom, there is a link that says "Did not receive the code? Resend code" with a person icon. A "Contact Us" link is located at the very bottom of the form.