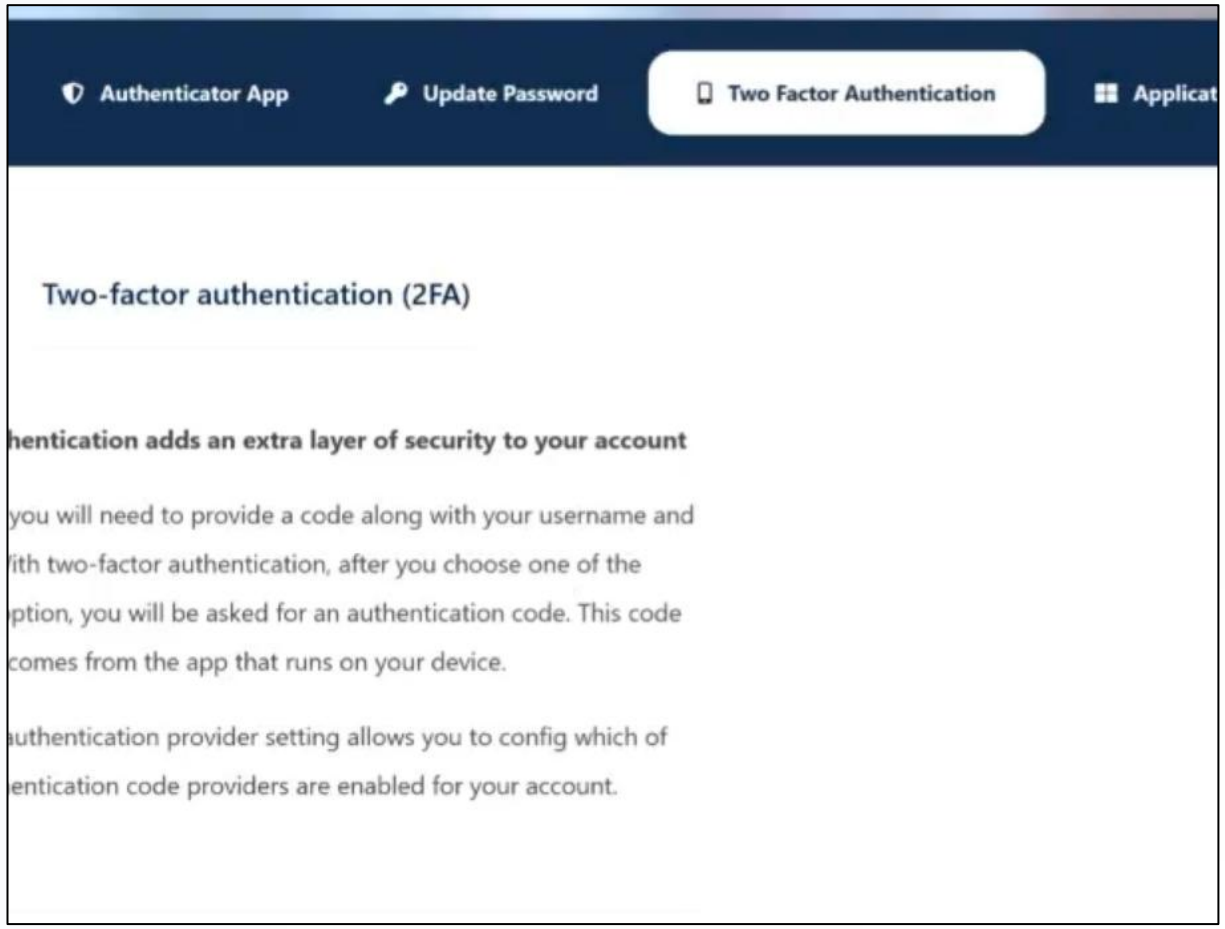
Two-Factor Authentication (2FA)

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.

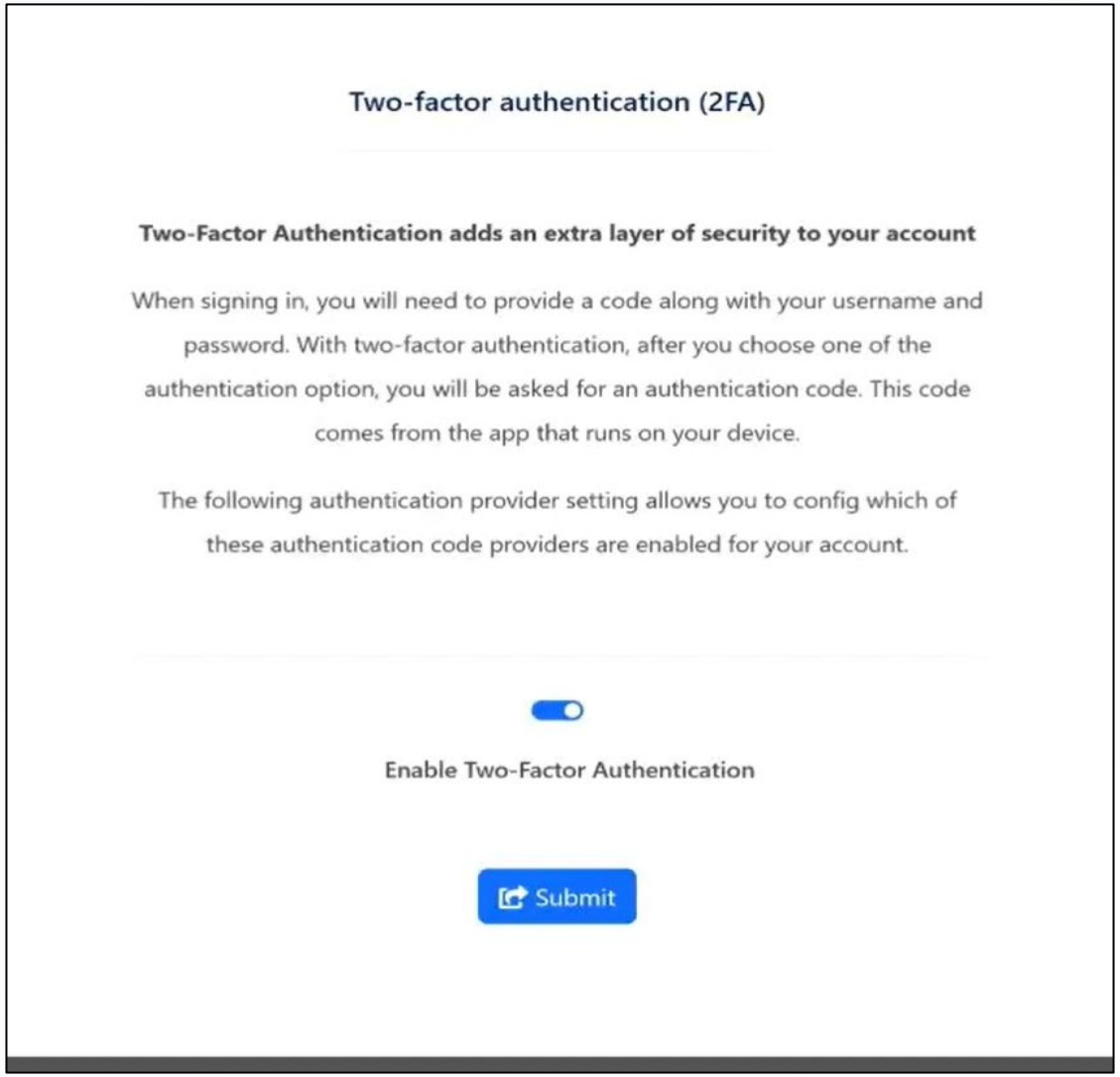


2. Enable & Submit

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

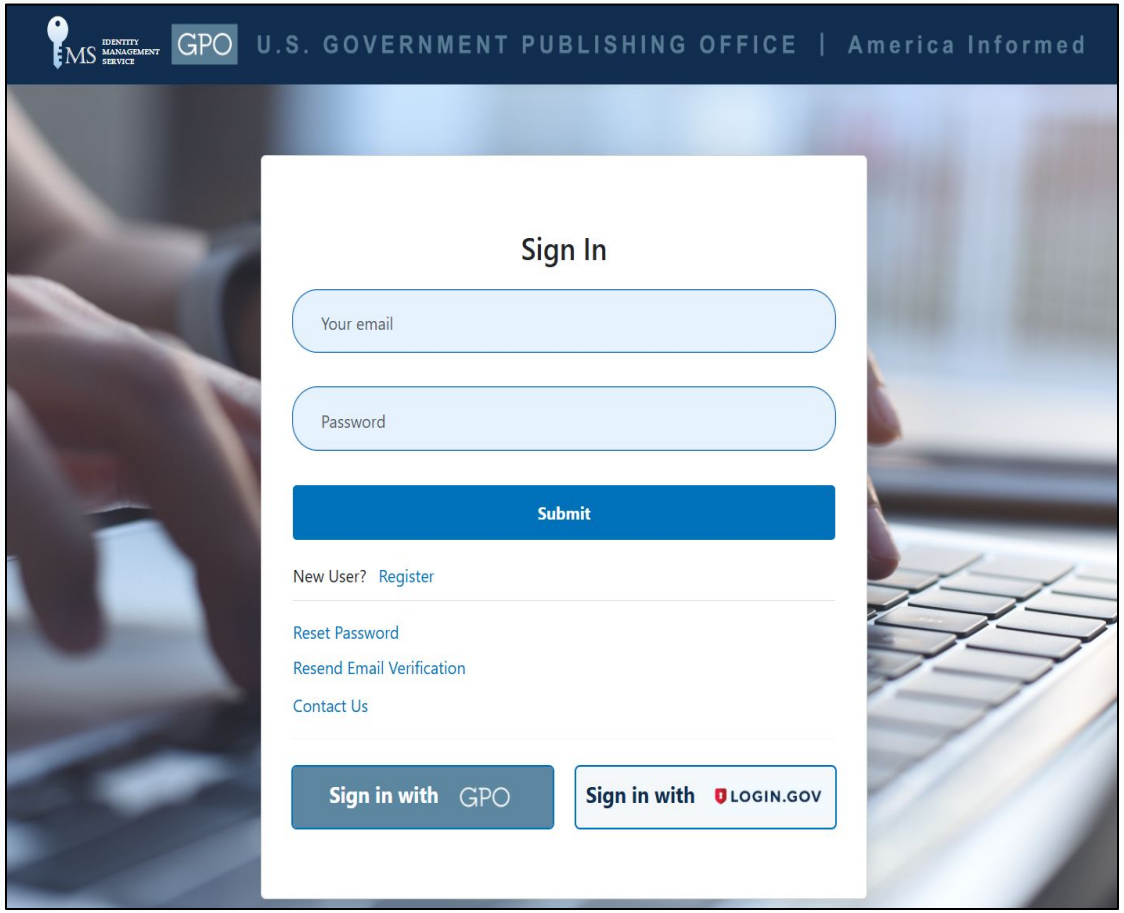
Generates real-time localized codes via standardized authenticator apps.

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.

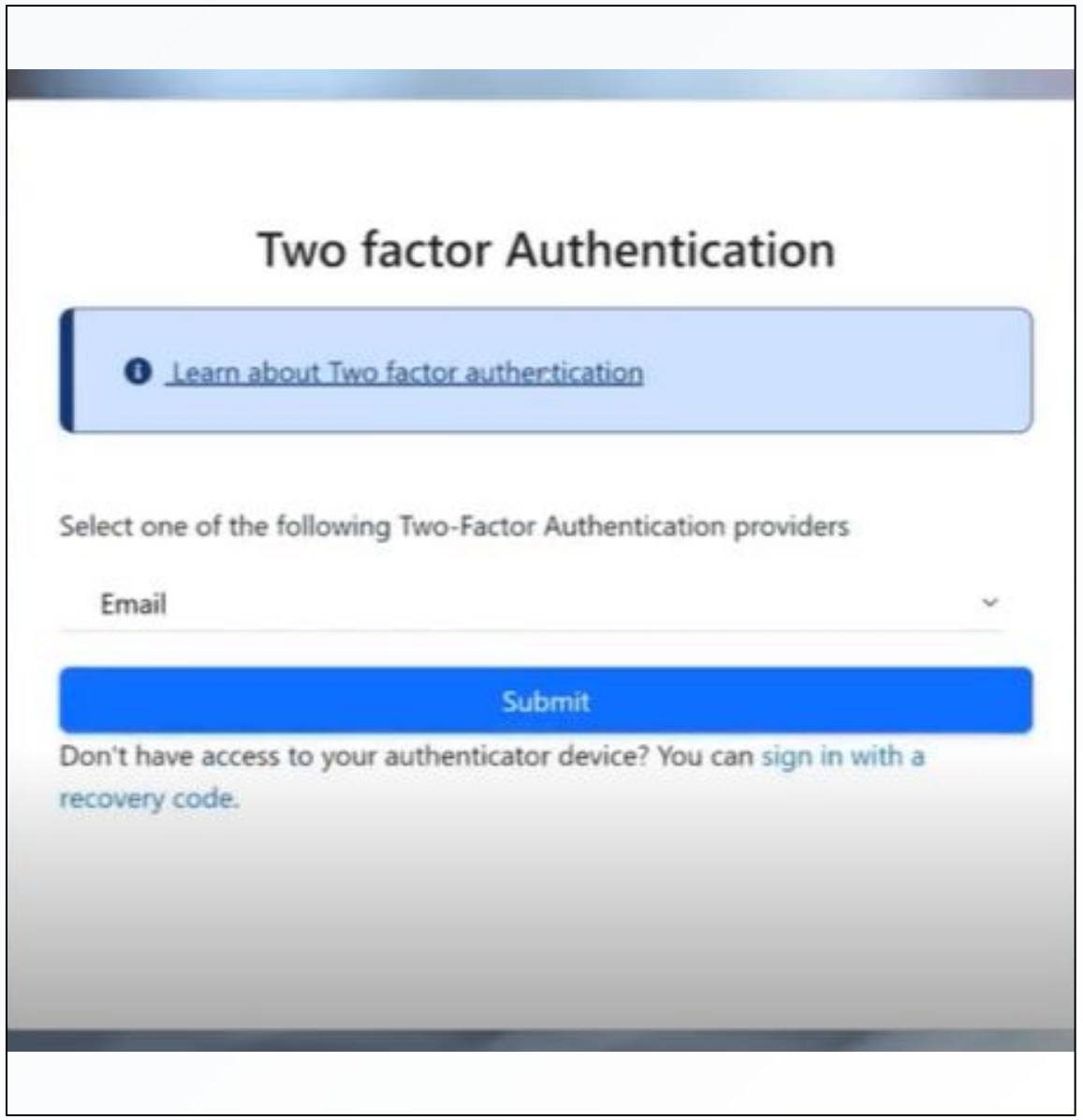


4. Select Delivery Method

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.



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.