How to Use 2FA

Two-factor authentication helps protect your HTAG account. It is optional for members and required for Board Admin accounts.

What is 2FA?

2FA means your password is not the only thing needed to sign in. After your password, the site may ask for a short code from an authenticator app on your phone.

1 Install an app

Use Google Authenticator, Microsoft Authenticator, Bitwarden Authenticator, 1Password, or any TOTP-compatible app.

2 Scan the QR code

Go to Account security, choose Set up 2FA, and scan the QR code shown on the HTAG page.

3 Save backup codes

When 2FA is enabled, copy or print the backup codes. Each backup code can be used once if you lose access to your phone.

Rules for HTAG accounts

Members may turn 2FA on for extra protection, but it is optional.

Board Admin accounts must turn on 2FA before using the admin area.

Board Admin accounts cannot disable 2FA once it is required.

Do not share your password, authenticator code, or backup codes with anyone.

HTAG does not use text message codes for admin 2FA. Use an authenticator app.

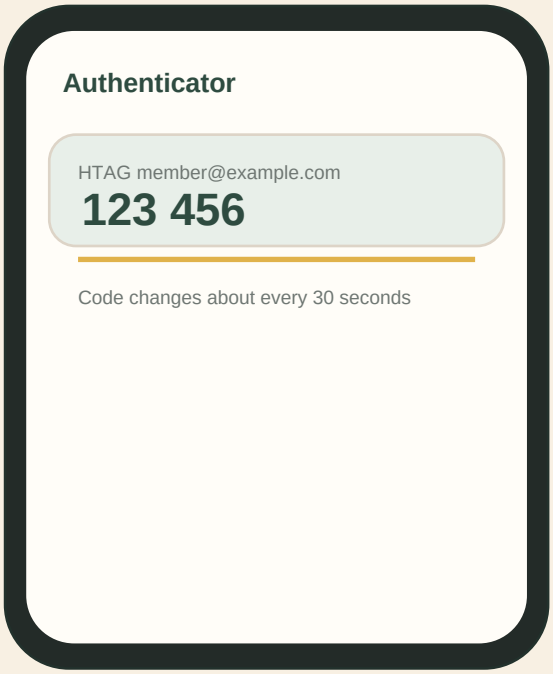
Before You Start

You only need a phone or tablet, an authenticator app, and access to your HTAG account.

Choose an authenticator app

- **Google Authenticator**
- **Microsoft Authenticator**
- **Bitwarden Authenticator**
- **1Password**
- **Any other TOTP-compatible authenticator app**

Download the app from your phone's app store before starting setup. The app will create a 6-digit code that changes often.



Important

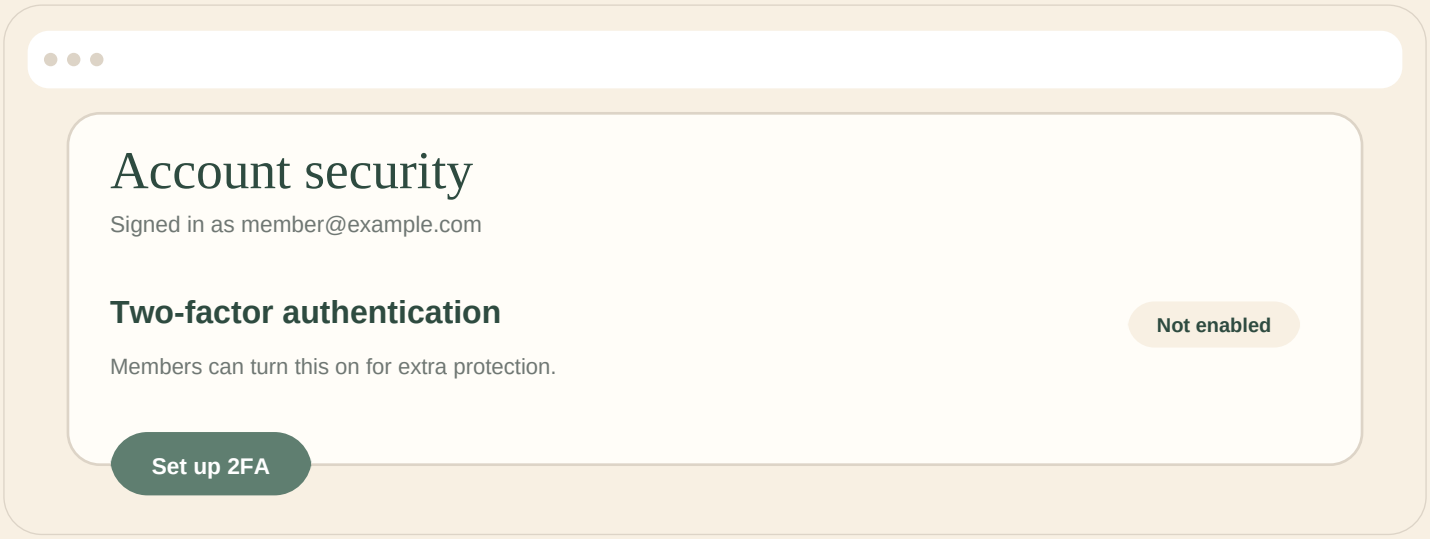
Do not delete the authenticator app entry after setup. If you delete it, you may need a backup code or help from HTAG leadership to get back in.

What you should have ready

- Your HTAG email and password
- Your phone or tablet
- An authenticator app installed
- A safe place to save backup codes

Turn On 2FA

Follow these steps while signed in to the HTAG website.



1 Open Account security

After signing in, go to Account, then open Account security.

2 Choose Set up 2FA

Click the Set up 2FA button. The website will show a QR code and a manual setup key.

3 Scan the QR code

Open your authenticator app and add a new account. Scan the QR code on the HTAG page. If scanning does not work, type the manual setup key into the app.

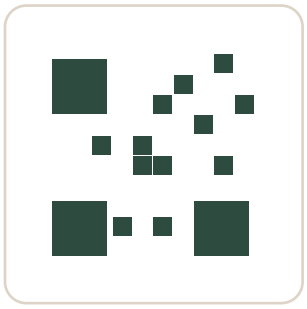
4 Enter the 6-digit code

Type the code from your authenticator app into the HTAG page and click Enable 2FA.

What You Will See During Setup

The real QR code and code numbers will be different for each person.

Two-factor authentication setup



Example QR code

Scan the QR code with your authenticator app. Then enter the 6-digit code it gives you.

Manual setup key

JBSWY3DPEHPK3PXP

Authenticator code

123456

Enable 2FA

About the 6-digit code

The authenticator code changes often. If the code fails, wait for the next code in the app and try again. Make sure your phone's time is set automatically.

After setup is enabled

The HTAG page will show backup codes. Copy, print, or save them somewhere safe before leaving the page. They will not be shown again.

Signing In With 2FA

Once 2FA is enabled, signing in has one extra step.

1 Enter email and password

Sign in to the HTAG website like normal with your email address and password.

2 Open your app

Open your authenticator app and find the HTAG entry for your account.

3 Type the code

Enter the current 6-digit code. Do not include spaces unless the website accepts them automatically.

4 Use backup code if needed

If you cannot access your authenticator app, use one saved backup code. Each backup code works one time only.

If the login code does not work

Wait for the next code in the authenticator app and try again.

Make sure you are using the HTAG entry in your authenticator app.

Make sure the phone or tablet time is set automatically.

Use a saved backup code if you no longer have access to the app.

Contact HTAG leadership if you are locked out and have no backup codes.

Backup Codes and Admin Notes

Backup codes are your emergency way back in if your authenticator app is not available.

How backup codes work

Backup codes are created when 2FA is turned on.

Each backup code can be used one time.

The codes are not shown again after you leave the page.

Store them somewhere safe, such as a password manager or printed copy.

You can create new backup codes from Account security after entering a valid authenticator or backup code.

Board Admin requirement

Board Admin accounts must use 2FA before accessing the admin area. Board Admin accounts cannot disable 2FA. This protects tenant records, documents, contact information, and administrative actions.

Final checklist

- [ ] Authenticator app installed
- [ ] 2FA enabled on the HTAG Account security page
- [ ] Backup codes saved somewhere safe
- [ ] Admin users confirm they can sign in before relying on the account for urgent work