

What Is an Authenticator App - and Why Should I Use One?

What is MFA?

Multi-Factor Authentication (MFA) adds a second step to your login (once every 30 days, depending on your preference). After your password, you confirm your identity with a short code. Think of it like a deadbolt - even if someone gets your key, they still can't get in. MFA is a vital step in keeping CHS MLS secure as scams advance in our industry.

What is an Authenticator App?

An authenticator app is a free app on your smartphone that generates a fresh 6-digit code every 30 seconds. When you log in, you open the app, read the code, and type it in. No text message or call needed.

Why is an authenticator app better than a text message?



- It is the most secure option.
- Text messages can be intercepted or lost in spam/unknown sender filters.
- Authenticator codes never leave your phone and expire every 30 seconds - nearly impossible to steal.
- Works without cell signal or Wi-Fi.

Most importantly – if you utilize an authenticator app for your CHS MLS MFA setup, MLS staff will have advanced options to help troubleshoot issues with you, should you ever have issues with your MLS password.

Which App Should I Use?

There is no specific authenticator app that you must use. They all fit the same purpose and it is completely up to you. Below are a few options, but choices are not limited to this list.

App	Best For	Available On
Google Authenticator	Most users — simple and easy	iPhone & Android
Microsoft Authenticator	Outlook / Office 365 users	iPhone & Android
Authy	Anyone who wants cloud backup across multiple devices	iPhone & Android
Duo Mobile	Users who prefer a one-tap "Approve" instead of typing a code	iPhone & Android
1Password	Users who already use 1Password as a password manager	iPhone & Android
1Password	LastPass password manager users	iPhone & Android
Apple Passwords (built-in)	iPhone users who already use Apple's Passwords Manager and want no extra app — built into iOS 18+	iPhone only

What Is an Authenticator App — and Why Should I Use One?

How Do I Set It Up?

If it's your first time logging into Flexmls and setting up your MFA -

1. Download the app of your choice from the App Store (iPhone) or Google Play Store (Android).
2. Log in to your MLS account and follow the MFA setup prompt. Choose "Authenticator App" as your method.
3. Scan the QR code shown on screen using the app (tap the "+" button, then "Scan a QR code").
4. Enter the 6-digit code from the app to confirm the connection. Done!

If you have already setup MFA, and need to CHANGE your MFA type -

1. Download the app of your choice from the App Store (iPhone) or Google Play Store (Android).
2. Navigate to Flexmls and choose Menu > My Profile > Security
3. Change the Code Delivery option to Authentication App, and click Save.
4. Scan the QR code that populates on screen using the app (tap the "+" button, then "Scan a QR code").
5. Enter the 6-digit code from the app to confirm the connection. Done!

What Does Logging In Look Like?

Don't forget – during this process you can select to “remember the device for 30 days” so that you can login without an MFA prompt for a longer stretch.

1. Enter your username and password.
2. Open the authenticator app on your phone.
3. Type in the 6-digit code shown.

Done - you're in!

Good to know:

- Don't delete the app - you'll need it every time you log in.
- Getting a new phone? Transfer your accounts before switching. Authy and Google Authenticator both have a built-in transfer option.
- Codes expire every 30 seconds - if you miss one, just wait for the next.
- No cell signal needed - the app generates codes offline.