How to Transfer Google Authenticator Codes to a New Device

TechRounder Help Center PDF

Live article: https://www.techrounder.com/help/how-to-transfer-google-authenticator-codes-to-a-new-device/

By Vipin PG | Published March 24, 2026 | Updated March 24, 2026 | Topic: Security | 3 min read

There are three methods depending on your situation: whether you have your old device available, whether your codes are synced to your Google Account, or whether you no longer have access to the old phone.

Method 1: Use Google Account Cloud Sync (Easiest - Recommended)

Since April 2023, Google Authenticator supports cloud backup to your Google Account. If you were signed in to the app on your old device, your codes are already backed up. Restoring them on a new device takes under a minute.

1. On your new device, install Google Authenticator from the App Store or Play Store.
2. Open the app and tap Sign in with Google .
3. Sign in with the same Google Account you used on the old device.
4. Your 2FA codes will automatically sync and appear in the app.

> Quote: Note: This only works if you were previously signed in to Google Authenticator with a Google Account on your old device. If you used the app without signing in (offline/local mode), use Method 2 below.

Method 2: Export via QR Code (Old Device Still Available)

If you still have your old phone and are not using cloud sync, use the built-in Export Accounts feature.

1. On your old device , open Google Authenticator.
2. Tap the three-dot menu (top right) and select Transfer accounts .
3. Tap Export accounts .
4. Verify your identity with biometrics or your PIN if prompted.
5. Select the accounts you want to transfer (you can select all), then tap Export . A QR code will appear on screen.
6. On your new device , install Google Authenticator, open it, and tap Get Started .
7. Tap Import existing accounts? , then tap Scan QR code .
8. Point your new device’s camera at the QR code displayed on the old device.
9. If you have more accounts than fit in one QR code, repeat the scan for each additional code shown.
10. Tap Done on the old device when finished.
11. Verify that codes are working on the new device before removing them from the old one.

> Quote: Important: Do not screenshot the QR code or share it with anyone. It contains the cryptographic seeds for all your 2FA accounts - anyone with this image can generate your codes.

Method 3: No Old Device and No Cloud Sync (Account Recovery)

If you lost your old device and did not have Google Account sync enabled, you must recover access to each service individually. You cannot recover Google Authenticator codes directly - the secrets existed only on the lost device.

1. For each account protected by Google Authenticator, go to that service’s login page on a computer.
2. Attempt to log in. When the 2FA prompt appears, look for an option like "Try another way" , "Use a backup code" , or "Can’t access your authenticator?"
3. Use a previously saved backup code (most services provide 8-10 single-use codes when you first set up 2FA) to log in.
4. Once logged in, navigate to the account’s Security or Two-Factor Authentication settings.
5. Disable the old authenticator and set up Google Authenticator fresh on your new device by scanning the new QR code provided by the service.
6. Save new backup codes and store them securely (a password manager is ideal).

For your Google Account specifically, visit myaccount.google.com/security, go to 2-Step Verification, and use a backup code or an alternative second factor (SMS, prompt on another signed-in device) to regain access.

Why This Happens

Google Authenticator generates time-based one-time passwords (TOTP) using a secret cryptographic seed stored on your device. Before the 2023 cloud sync update, these seeds existed only locally - there was no backup by default. This meant losing your device locked you out of every account using Authenticator unless you had backup codes saved. The Export/Import QR code method was the only built-in migration path. Cloud sync now solves this for users signed in with a Google Account, but those running the app in offline mode are still subject to the old limitation.

Security Note on Cloud Sync

Google’s cloud sync feature does not yet use end-to-end encryption (E2EE) by default. This means Google can technically access your 2FA seeds in the event of a breach or legal request. For higher security, consider using an alternative app such as Aegis (Android, open source, E2EE local backup) or Raivo (iOS, encrypted vault). If you continue with Google Authenticator’s cloud sync, ensure your Google Account itself is secured with a strong password and a separate second factor.

Official sources and references

1. myaccount.google.com - security - https://myaccount.google.com/security