

Phone upgrade: authenticator checklist

Complete every step before you factory reset your old phone.

1. List every account that uses the authenticator

- ☐ Open the authenticator app and write down every entry you can see.
Scroll the full list, some apps hide entries behind a dropdown.
- ☐ Microsoft 365 or work email
- ☐ Google account, personal and work
- ☐ Password manager
- ☐ Accounting or invoicing software
- ☐ Cloud storage (OneDrive, Dropbox, Google Drive)
- ☐ Social media accounts with MFA enabled
- ☐ Any line of business app your organisation uses

2. Check whether your app can back up

- ☐ Microsoft Authenticator: back up to a personal Microsoft account.
Work and school accounts are not always included, check the backup screen.
- ☐ Google Authenticator: sync codes to your Google account.
- ☐ Authy: cloud backup protected by a backup password.
- ☐ Turn the backup on, confirm it has synced, then test the restore on the new phone.

3. Move each account, one at a time

- ☐ Log in on a computer and open the security or two-factor settings.
- ☐ Add a new authenticator method, or replace the existing one.
- ☐ Scan the QR code with the app on the new phone.
- ☐ Log in once using a code from the new phone to confirm it works.
- ☐ Only then remove the old phone from that account.

4. Before you reset the old phone

- ☐ Confirm a recovery email and phone number are set on every account.
- ☐ Save or print any backup recovery codes the account gave you.
- ☐ Keep the old phone charged and enrolled for one week.
- ☐ After a week of clean logins on the new phone, reset the old one.

Already locked out?

Contact your tenant administrator for Microsoft 365 and Google Workspace accounts. If you are a Live IT client, that is me, get in touch and I will reset it for you. For everything else, use the provider's own account recovery flow and expect to prove your identity.