Microsoft Accounts, Passwords & MFA (Microsoft Entra ID) — Complete End-User Guide

> For employees/students using a work or school Microsoft 365 account. This manual explains exactly **where to sign in**, **how to change or reset your password**, **how to set up and use MFA (Microsoft Authenticator, phone, passkeys/security keys)**, and **how to fix common sign-in issues**—plus an escalation checklist. Admin-only notes are clearly marked.

---

0) What this covers

- What “Microsoft account,” “work/school account,” and **Entra ID** mean
- Where to sign in for email, apps, and account settings
- Change password vs. reset password (locked/forgot)
- Registering/using **Microsoft Authenticator**, phone codes, **passkeys** and **security keys (FIDO2)**
- Typical sign-in/MFA problems and exact fixes (loops, code failures, device time, old Outlook profiles)
- Moving to a new phone safely (without lockouts)
- Legacy app scenarios (IMAP/SMTP, POP, older devices)
- When/how to escalate

---

1) Key concepts in 90 seconds

- **Work or school account**: Your org-managed Microsoft identity (e.g., you@company.com) hosted in **Microsoft Entra ID** (formerly Azure AD).
- **Password change**: You know your current password and want to change it.
- **Password reset (SSPR)**: You forgot your password or your account is locked; you'll prove who you are with your registered methods, then set a new password.
- **MFA (multi-factor auth)**: A second step after your password—typically **Microsoft Authenticator push**, a **one-time code**, **text/voice**, or a **security key**/**passkey**.
- **Methods**: You should register **at least two** methods (e.g., Authenticator + phone or security key) so you're never locked out.

---

2) Where to sign in (and what for)

- **Email & calendar (web):** `https://outlook.office.com`
- **Microsoft 365 portal (apps & files):** `https://office.com` (click **Outlook**, **OneDrive**, **Teams**, etc.)
- **Account & security settings:** `https://myaccount.microsoft.com` → **Security info**, **Devices**, **Privacy**
- **Self-service password reset:** `https://passwordreset.microsoftonline.com`

Tip: Bookmark those four. They solve 90% of "where do I go?" questions.

---

3) Changing your password (you still remember it)

Option A — From the web (works anywhere)

1. Go to `https://myaccount.microsoft.com`.
2. Open **Security info** (or **Password**) → **Change password**.

3. Enter current password → set a new one (follow your org's rules: length, complexity, history).

4. After changing, **sign out & back in** on Outlook/Teams/OneDrive and your mobile apps. If a desktop Outlook profile keeps prompting, see **§9.3**.

Option B — From a Windows work PC (domain/Entra-joined)

1. Press **Ctrl + Alt + Delete** → **Change a password**.

2. Lock/unlock once, then sign out/in in Office apps on that device and your phone.

> Good practice: Rotate passwords during work hours (not at night) so support can help if anything goes wrong.

---

4) Resetting your password (forgotten or locked)

Self-Service Password Reset (SSPR)

1. Go to `https://passwordreset.microsoftonline.com`.

2. Enter your work/school email → follow prompts (Authenticator approval or a code to your registered methods).

3. Set a **new** password.

4. Re-sign in on all devices. If Outlook keeps looping on one PC, see **§9.3**.

If SSPR says you're not registered: go to **§5** to register methods first (you'll need to contact your helpdesk this one time if you're already locked out and unregistered).

---

5) Register your sign-in methods (do this now, not later)

5.1 Open your Security info page

- Go to `https://myaccount.microsoft.com` → **Security info** → **Add method**.
- Register **at least two** of the following: **Microsoft Authenticator**, **Phone**, **Email** (if your org allows), **Security key (FIDO2)**, or **Passkey**.

5.2 Microsoft Authenticator (recommended default)

1. Install **Microsoft Authenticator** on iOS/Android.
2. In **Security info** → **Add method** → **Authenticator app** → **Next**.
3. Scan the QR code from your phone → approve a test notification.
4. You'll get **push approvals** or **number matching** prompts at sign-in.

Tips

- Keep **notifications enabled** and **time/date set to automatic** on your phone.
- Add a **second method** (phone or security key) in case you lose your phone.

5.3 Phone (text/voice) as a backup

1. **Add method** → **Phone** → enter number.
2. Choose **Text me a code** or **Call me**.
3. Verify the code or call.

5.4 Security keys (FIDO2) and Passkeys (phishing-resistant)

- **Security key (FIDO2)**: A physical USB-A/USB-C/NFC/BLE key (e.g., YubiKey).
    1. **Add method** → **Security key** → choose **USB** or **NFC**.
    2. Insert/tap key when prompted → create a **PIN** for the key (not your account password) → register.

- **Passkey**: A platform-stored credential protected by device biometrics/PIN (supported browsers/devices).

    1. **Add method** → **Passkey** (if available) → follow prompts to create on your PC/phone.

- Use these when traveling or where push approvals might be unreliable.

5.5 TOTP codes (backup even without data)

- In Authenticator, you can view **6-digit codes** that work offline. If codes fail: ensure **automatic time** is enabled on your phone.

---

6) Good hygiene & policy basics

- **Have two methods** minimum (ideally Authenticator **and** a security key/phone).
- **Don't share** your password or approval codes—ever. No one from IT will ask.
- **New phone?** Add the new Authenticator **before** wiping the old one (see **§8**).
- Use **passkeys/security keys** for sensitive roles if your org supports them.
- **Sign-in frequency** prompts depend on policy; choose **"Don't show again"** only if allowed.

---

7) Everyday sign-in (what you'll see)

1. Enter your work email at a Microsoft sign-in page.
2. Enter your password (or use a passkey/security key if configured).
3. Complete MFA:

- **Authenticator**: You'll see a number on the sign-in screen; open the app and tap the same number (number matching).
- **Code**: Enter the 6-digit code from Authenticator or SMS.
- **Security key**: Touch/tap the key and enter its PIN when asked.

If you check **"Stay signed in"**, you may sign in less often (depends on org policy).

---

8) Moving to a new phone (avoid lockouts)

Before you factory-reset or discard the old phone:

1. On a computer, go to `https://myaccount.microsoft.com` → **Security info**.
2. **Add method** → register the **new** Authenticator (scan QR), **OR** temporarily add **Phone**/Security key.
3. Verify you can approve sign-ins using the **new** method.
4. Remove the **old** phone entry.
5. Only now wipe or discard the old device.

Lost or stolen phone?

- If you still have access to another method (e.g., text or security key), sign in and **remove** the lost phone from **Security info** ASAP. Then add your replacement method.

---

9) Troubleshooting (symptom → fix)

9.1 "I can't sign in—MFA push never arrives"

- Ensure the phone is online and **notifications** are enabled for Authenticator.
- Open Authenticator to see pending requests; try **Use a verification code** instead.

- If codes fail, set **Automatic date & time** on the phone.
- Try a backup method (text/voice, security key).
- If nothing works and you have no backup method, **contact IT** to restore access.

9.2 “I changed my password; now apps keep prompting”

- Sign out/in once in **Outlook**, **Teams**, **OneDrive** (desktop & mobile).
- On Windows Outlook (classic) if loops persist: **File** → **Account Settings** → **Remove** the account and re-add; or **rebuild your Outlook profile** (Control Panel → Mail → Show Profiles → Add → set default).
- On macOS Outlook: add the account again; if stuck, create a new profile via **Outlook Profile Manager**.

9.3 “Outlook keeps asking for my password/MFA in a loop”

- Make sure the **OS time** is correct (automatic).
- Complete any **stuck MFA** prompts first (open Authenticator directly).
- **New profile** usually fixes the loop (see §9.2).
- If VPN forces all traffic and blocks Microsoft endpoints, connect **after** initial sign-in (unless your org requires VPN first) or switch temporarily to a non-VPN network to complete login.

9.4 “My Authenticator codes are ‘incorrect’”

- Phone time must be **automatic**; for big drift, restart the phone.
- Re-register the Authenticator method from **Security info** if it’s out of sync.

9.5 “My account is locked”

- Use **SSPR**: `https://passwordreset.microsoftonline.com`.

- If SSPR says you're not registered, contact your helpdesk; after unlock, **register methods** immediately (see §5).

9.6 "I got an MFA prompt I didn't request"

- **Deny it.** Change your password right away and notify IT/security.
- Consider enabling a **security key/passkey** method, which is phishing-resistant.

9.7 "Keep asking for sign-in every day"

- Your **Sign-in frequency** policy may require it (security setting).
- If allowed, check **Stay signed in** at login.
- Avoid clearing cookies for Microsoft sites; exclude them from browser cleaners.

9.8 "I need mail on an old device / legacy app"

- Many orgs disable **basic auth** (POP/IMAP/SMTP AUTH) for security.
- Use the **Outlook** app or a client that supports modern auth.
- If legacy access is truly needed, ask IT; they may offer app-specific alternatives or service accounts with conditional access controls.

---

10) Advanced options (power users & recommended defaults)

10.1 Priority of methods

- In **Security info**, you can set a **Default sign-in method** (e.g., Authenticator notification). Keep at least **one backup** registered.

10.2 Security keys & passkeys (best friction-to-security ratio)

- Use a **USB-C or NFC key** if you roam between devices or travel often.
- For laptops with Windows Hello/Touch ID: create a **passkey** and use your device biometrics at sign-in.

10.3 App passwords (legacy)

- Typically **not allowed** in modern orgs. Only use if IT explicitly enables and instructs you (e.g., a single legacy device). Replace with modern clients ASAP.

10.4 Name changes, aliases, mailbox moves

- If your sign-in name changes (e.g., marriage), you'll keep access but may be asked to sign in again. Update your **aliases** and **primary SMTP** via the helpdesk as per policy.

---

11) Security best practices (user actions)

- **Never approve** an MFA prompt you didn't initiate.
- **Unique password**: don't reuse your corporate password anywhere.
- Prefer **Authenticator push** or **security keys/passkeys** over SMS (more secure).
- Keep your phone number and recovery methods **current**.
- When traveling, bring a **backup method** (second device or key).

---

12) Common helpdesk ticket patterns → quick fixes

Symptom in tickets	Root cause (typical)	Do this first	If still failing
"MFA prompt never comes"	Phone notifications off / no data	Open Authenticator, use code; enable notifications; try Wi-Fi/cellular	Use backup method; re-register method

“Outlook asks for password repeatedly”	Token stale / profile glitch	Sign out/in; complete MFA in Authenticator	Rebuild Outlook profile; check OS time
“Forgot password, can’t log in”	Not registered for SSPR	Use SSPR if registered	Helpdesk unlock; then register 2+ methods
“New phone; locked out”	Old phone wiped first	Add new method **before** wiping old	Helpdesk resets methods; re-register
“Suspicious MFA prompts”	Stolen password/phishing	Deny, change password, notify security	Add security key/passkey; phishing training
“Need email on old device”	Basic auth disabled	Use Outlook app / modern client	Helpdesk for exceptions, or service account

---

13) Escalation checklist (what IT needs to help fast)

- **Your info**: Name, department, time zone, a callback number.
- **Scope**: Is anyone else affected? (names/emails)
- **Exact error**: Screenshot or the full error text.
- **When it started** and **what changed** (password, phone, OS update, new device, VPN change).
- **Tried so far**: SSPR, alternate method, sign out/in, new Outlook profile, device time set to automatic.
- **Device/app details**: Windows/macOS/iOS/Android versions; Outlook type (new vs classic); browser used.

---

14) Quick reference: one-liners you can paste into replies

- **Change password**: `myaccount.microsoft.com` → **Security info** → **Change password**
- **Forgot password**: `passwordreset.microsoftonline.com`
- **Add methods**: `myaccount.microsoft.com` → **Security info** → **Add method** (Authenticator + Phone + Security key/passkey)
- **New phone**: Add the **new Authenticator** first → remove the old phone
- **MFA not arriving**: Open Authenticator → use code; ensure notifications & automatic time; try backup method
- **Outlook loop**: Sign out/in → rebuild profile if needed

Final notes

- Screens may differ slightly based on your company's policy and app version; the names above will still find the right pages via the **Settings/Search** bars.
- Keep two active methods at all times. Add a security key or passkey if available for best security with minimal friction.