Two Factor Authentication

PatchMon supports time-based one-time password (TOTP) two-factor authentication (2FA, sometimes called MFA) on top of the normal username / password login. Once enabled on a user's account, every sign-in asks for a 6-digit code from an authenticator app, or a one-time backup code.

This page covers enabling 2FA per user, using backup codes, the "Remember Me" trusted-device feature, and how admins recover an account if the user loses their authenticator.

> **Related pages:**
>
> - Users, Roles and RBAC: manage user accounts
> - Setting Up OIDC / Single Sign-On: delegate authentication to an external IdP
> - PatchMon Environment Variables Reference: the full env-var list

---

Scope and limitations

- 2FA is **opt-in per user**. Each user decides whether to turn it on from their own profile.
- 2FA is **not available for OIDC accounts.** If a user signs in via OIDC / SSO, their IdP is responsible for MFA. The PatchMon TFA tab is hidden on the profile page for OIDC-only accounts, and the setup endpoint refuses with "*MFA is managed by your OIDC provider*".
- There is **no global "require 2FA for all users"** flag in the current release. Administrators cannot enforce 2FA for every account from the UI or an environment variable. If you need enforced 2FA, drive authentication through an OIDC provider that enforces MFA (e.g. Authentik, Entra ID) and set `OIDC_DISABLE_LOCAL_AUTH=true`.
- The first-time setup wizard offers new admins the option to set up 2FA during initial account creation (Step 2 of the wizard). This is voluntary and can be skipped.

Enabling 2FA on Your Account

Each user enables 2FA themselves from their profile. Admins cannot enable it on behalf of another user.

1. Sign in to PatchMon with your username and password.
2. Click your avatar (top-right) → **Profile**.
3. Open the **Multi-Factor Authentication** tab.
4. Click **Enable TFA**.
5. A QR code appears. Scan it with your authenticator app of choice. Known-good options:
   - **Authy**
   - **Google Authenticator**
   - **1Password**
   - **Bitwarden**
   - **Microsoft Authenticator**
   - **Duo Mobile**
6. If you can't scan the QR code (shared device, desktop-only app), copy the **Manual Entry Key** instead and paste it into your authenticator.
7. Click **Continue to Verification**.
8. Enter the current 6-digit code from your authenticator app.
9. Click **Verify & Enable**.

You are now shown a one-time list of **backup codes** (see next section). Save them before clicking **Done**.

From now on, every password-based login will prompt for a 6-digit verification code after the password step.

Backup codes: save these

After enabling 2FA, PatchMon generates a batch of single-use backup codes. These let you sign in if you lose access to your authenticator app (lost phone, wiped device, etc.).

- **Each code can be used exactly once.** Once used, it is consumed and cannot be reused.
- **They are shown only once**, in plaintext, immediately after setup or regeneration. PatchMon stores them as bcrypt hashes in the database; neither you nor an admin can recover the plaintext later.
- **Treat them like a second password.** Store them in a password manager, or print them and lock them away.
- Click **Download Codes** to save a plain-text file for offline storage.

Regenerating backup codes

If you think your backup codes have leaked, or you've used most of them:

1. Go to **Profile → Multi-Factor Authentication**.
2. Scroll to the **Backup Codes** panel.
3. Click **Regenerate Codes**.

4. A new set of codes is generated and shown. The old set is immediately invalidated.

Using a backup code

On the 2FA prompt at login, you enter backup codes in the **same field** as TOTP codes. There is no separate "use a backup code" button. PatchMon tries the code as a TOTP first; if that fails, it checks whether it matches one of the stored backup-code hashes. If it matches, that backup code is consumed (removed from the stored list) and you are logged in.

Typical workflow if you've lost your phone:

1. At the login page, enter your username and password as usual.
2. On the "Two-Factor Authentication" screen, type one of your backup codes in the **Verification Code** field.
3. Click **Verify**.

The code is spent. Your next login cannot use the same backup code again.

"Remember Me": Trusted Devices

When you enter your 2FA code, there's a **Remember me on this computer (skip TFA for 30 days)** checkbox. If ticked, PatchMon plants a long-lived, HttpOnly `patchmon_device_trust` cookie on that browser and records a hashed trust token in the database.

On subsequent logins from the same browser:

- You still enter your password.
- PatchMon sees the trust cookie, matches it to the database record, confirms the record belongs to you and hasn't expired, and skips the 2FA prompt.
- A `last_used_at` timestamp on the trust record is bumped each time it's used, so you can see when each remembered device last signed in.

How the trust is keyed

The trust cookie is keyed only on **(user ID, cookie hash)**. It is deliberately **not** bound to IP address or user agent, so:

- Roaming between Wi-Fi, mobile hotspot, and office network does not invalidate the trust.
- Updating your browser does not invalidate the trust.
- Copying the cookie to a different browser on a different machine **would** bypass 2FA for that user (standard web cookie security model). Protect your browser profile accordingly.

Trust lifetime

The default lifetime is **30 days**, configurable server-wide via the `TFA_REMEMBER_ME_EXPIRES_IN` environment variable. Accepts duration strings such as `7d`, `30d`, `90d`. See PatchMon Environment Variables Reference for the full list.

There is a hard cap on how many trusted devices a single user can accumulate, controlled by `TFA_MAX_REMEMBER_SESSIONS` (default `5`). When a sixth device is trusted, the oldest existing trust is removed automatically.

Reviewing your trusted devices

1. Go to **Profile → Trusted Devices**.
2. You'll see a list with, for each device:
   - **Label** (best-effort device name derived from the user agent)
   - **User agent**
   - **IP address** at the time it was last used
   - **Created** / **Last used** / **Expires** timestamps
   - A **This device** badge next to the one you're currently logged in from

Revoking a trusted device

To stop a specific device skipping 2FA (for example, an old laptop you're decommissioning):

1. **Profile → Trusted Devices**.
2. Find the device in the list and click **Revoke**.
3. Confirm.

If the device you're revoking is the **current** browser, its trust cookie is also cleared, so your next login from this browser will require 2FA again.

Revoking every trusted device

Click **Forget all trusted devices** at the top of the panel. This:

- Removes every trust record for your account.
- Clears the trust cookie on the current browser.
- Forces a full 2FA prompt on every device next time you sign in.

Use this after a suspected account compromise or after losing a device.

Disabling 2FA

To turn 2FA back off on your own account:

1. **Profile → Multi-Factor Authentication**.
2. Click **Disable TFA**.
3. Enter your password to confirm.
4. Click **Disable TFA**.

Side effects:

- The TOTP secret is wiped from the database.
- All existing backup codes are invalidated.
- **All of your trusted devices are revoked.** This is intentional. The only purpose of a trust record is to skip 2FA, so with 2FA off they serve no purpose. If you later re-enable 2FA, old trust cookies will not be resurrected and every device must confirm 2FA again.

> You cannot disable 2FA on an OIDC-only account. The API rejects the request with "*Cannot disable TFA for accounts without a password*". This is because disabling 2FA requires password confirmation, and OIDC-only accounts have no password set.

Failed Attempts and Lockout

To prevent brute-forcing the 6-digit code space, the verify-2FA endpoint is rate-limited per user.

Env var	Default	What it does
`MAX_TFA_ATTEMPTS`	`5`	Consecutive wrong codes allowed before a lockout
`TFA_LOCKOUT_DURATION_MINUTES`	`30`	How long the lockout lasts

After the cap is hit, the endpoint returns HTTP `429 Too Many Requests` with the message "*Too many failed TFA attempts. Please try again later.*" Wait out the lockout, or ask an admin (see below).

Each failure also returns a `remainingAttempts` counter in the response, so the login UI can tell the user how many tries are left.

First-Time Wizard: Optional 2FA Setup

When you bring up a brand-new PatchMon instance and complete the setup wizard, **Step 2 (Multi-Factor Authentication)** offers two choices:

- **Setup MFA now:** scan a QR code and register an authenticator for the brand-new admin account before finishing the wizard. You'll also capture your backup codes.
- **Skip for now:** the admin account is created without 2FA. You can turn it on later from **Profile → Multi-Factor Authentication**.

There is no "enforce for everyone" option in the wizard. This decision is always per-user.

Admin Recovery: User Has Lost Their Authenticator

PatchMon does not have a dedicated "admin reset MFA" button. Recovery is handled through the standard account-recovery flow, which implicitly disables 2FA in a safe way:

Option A: User has a backup code

Ask them to sign in with a backup code (see Using a backup code). Once they're in, they can:

1. **Profile → Multi-Factor Authentication → Disable TFA** to remove the old authenticator secret entirely, and then re-enable with the new phone.
2. Or **Regenerate Codes** to get a fresh set of backup codes without touching the authenticator.

Option B: User has no backup codes and no authenticator

An administrator must reset the account:

1. Sign in as a user with `can_manage_users` (admin, superadmin, or any custom role with that permission).
2. Go to **Settings → Users**.
3. Find the affected user and click **Reset Password**.
4. Set a new password and communicate it over an out-of-band secure channel.

> **Password reset alone does not disable 2FA.** The user will still be prompted for a TOTP or backup code after their first login with the new password.

If the user still cannot produce a code, you have two further options:

- **Deactivate, then reactivate the account.** Edit the user, untick **Active**, save (this also wipes their trusted devices), then tick **Active** again. 2FA is still enabled on the account, so this alone does not solve the missing-authenticator problem.
- **Delete and re-create the user** as a last resort. You lose the user's ID, notification preferences, and any artefacts keyed to their account, so prefer the backup-code route wherever possible.

> **Feature gap:** A "wipe 2FA on another user" admin action is on the roadmap. If you hit this frequently, consider moving your deployment to OIDC / SSO so that MFA is managed by the IdP (see Setting Up OIDC / Single Sign-On).

Direct database workaround (self-hosted only)

If you are self-hosting and absolutely need to clear 2FA on a user without backup codes, a DBA can clear the user's `tfa_enabled`, `tfa_secret` and `tfa_backup_codes` columns directly in the `users` table, then force a password reset from the UI. This is a last resort. Make a backup first, and never do this on PatchMon Cloud (where direct database access is not available).

```
-- Replace 'alice' with the affected username. Make a backup first.
UPDATE users
SET tfa_enabled = false,
    tfa_secret = NULL,
    tfa_backup_codes = NULL
WHERE username = 'alice';
```

After running this the user can sign in with just a password; they should immediately re-enrol in 2FA from their profile.

Environment Variables Reference

All of these are read once at server start. Changes require a restart to take effect. The full table lives in PatchMon Environment Variables Reference; reproduced here for convenience:

Variable	Default	Description
`MAX_TFA_ATTEMPTS`	`5`	Consecutive wrong 2FA codes before the account is temporarily locked
`TFA_LOCKOUT_DURATION_MINUTES`	`30`	How long a 2FA lockout lasts
`TFA_REMEMBER_ME_EXPIRES_IN`	`30d`	How long a "Remember me" trusted-device record is valid. Accepts `7d`, `30d`, `90d`, etc.
`TFA_MAX_REMEMBER_SESSIONS`	`5`	Maximum number of trusted devices per user; the oldest is evicted when the limit is reached

---

Troubleshooting

"Invalid verification code" when I know the code is correct

1. **Clock skew.** TOTP codes are time-based. If your phone's clock is more than ~30 seconds out of sync with the server, codes will be rejected. Enable automatic date/time on your phone. PatchMon already tolerates a small drift window server-side, but not more than that.
2. **Using a used code.** TOTP codes roll every 30 seconds. If you paste a stale code from 60+ seconds ago it will fail. Wait for a fresh code.
3. **Used backup code.** Backup codes are single-use. If you've already used one, try a different one.

"Too many failed TFA attempts"

You've hit `MAX_TFA_ATTEMPTS`. Wait `TFA_LOCKOUT_DURATION_MINUTES` (default 30) and try again. There is no admin "unlock" button; the lockout key in Redis expires automatically. Self-hosters can flush the key by restarting Redis.

I ticked "Remember me" but I'm still being asked for 2FA

Three likely causes:

- The trust record has expired. The default lifetime is 30 days; check `TFA_REMEMBER_ME_EXPIRES_IN` on your server.

- You're signing in on a different browser, or in a private / incognito window, which doesn't have the cookie.
- A password reset was performed on your account. Password resets (whether self-service or admin-initiated) revoke every trusted device as part of the security response. You'll need to tick **Remember me** again on the next 2FA prompt.

My MFA tab is missing on the profile page

You signed in via OIDC. PatchMon defers MFA to your IdP in that case. Enable MFA in your IdP (Entra ID, Authentik, Keycloak, etc.) if you want it.

I regenerated backup codes but the old ones still work

The old codes are invalidated at the same moment the new batch is displayed. If a stale code still seems to work, make sure you're looking at the right account. Backup codes are not user-transferable.

Revision #1
Created 2026-04-25 10:15:46 UTC by Iby
Updated 2026-04-25 10:15:57 UTC by Iby