

Turn on two-step sign-in

Make everyone confirm their sign-in with a code from an app on their phone. Set up your own first, then your team is walked through it the next time they sign in.

Setup guide · For Owners, Managers, Everyone on the team · aminova.health/university/two-step-sign-in

1. WHAT TWO-STEP SIGN-IN IS

Two-step sign-in means a password alone can't open your clinic's Aminova. After the password, each person types a 6-digit code from an authenticator app on their phone. The code keeps changing, so a stolen password isn't enough.

It is on for every clinic from the start. Nobody gets locked out by it: anyone who hasn't set it up is walked through it the next time they sign in.

2. GET AN AUTHENTICATOR APP

Each person needs a free authenticator app on their phone. Any of the common ones works. Install it from your phone's app store before you start.

3. CHECK IT'S REQUIRED

1. Go to **Settings**, then **Security**.
2. Under **Two-Factor Authentication**, make sure **Require 2FA for all staff** is switched on.
3. It saves on its own.

The screenshot displays the 'SECURITY CONFIGURATION' page in the Aminova interface. A sidebar on the left contains links to 'Patient Portal', 'Security' (highlighted), 'Integrations', 'HIPAA & Compliance', 'Data & Privacy', 'Roles & Permissions', and 'AI Scribe'. The main content area has a yellow header bar with the title 'SECURITY CONFIGURATION' and a 'Partially configured' status indicator. Below this, a progress bar shows the configuration status of various security features. The 'Two-Factor Authentication' section is highlighted with a blue border and contains a toggle for 'Require 2FA for all staff' which is turned on. Below the toggle, it states 'Providers, admins, and support staff verify with a one-time code on login'. There is also a 'Your authenticator' section with a 'Set up' button. At the bottom, there are three dropdown menus: 'Session Timeout' set to '60 minutes', 'Lock After N Failures' set to '5 attempts', and 'Lockout Duration' set to '30 minutes'. Below these are labels for 'Auto-logout after inactivity', 'Failed attempts before lockout', and 'How long the account stays locked'. A 'Trusted IP Ranges' section is also visible at the bottom.

Feature	Status
Staff 2FA required	✓
Login lockout active	✓
Session timeout set	✓
Trusted IP ranges set	✗

Two-Factor Authentication

Require 2FA for all staff ☒

Providers, admins, and support staff verify with a one-time code on login

Your authenticator

Required by your clinic — set it up now

Session Timeout 60 minutes

Auto-logout after inactivity

Lock After N Failures 5 attempts

Failed attempts before lockout

Lockout Duration 30 minutes

How long the account stays locked

Trusted IP Ranges

Require 2FA for all staff, with your own authenticator just below it.

4. SET UP YOUR OWN

1. Just below, find **Your authenticator** and press **Set up**.
2. Open the authenticator app on your phone, add an account, and scan the square code on screen.
3. Can't scan it? Click **Can't scan? Enter the key manually** and type the key into the app instead.
4. Type the 6-digit code the app shows, then press **Verify & enable**.

5. SAVE YOUR BACKUP CODES

1. Next you see a list of backup codes. They are shown only this once.
2. Press **Copy all** and keep them somewhere safe, away from your phone, like a password manager or a locked drawer.
3. Each code works one time, if you ever lose your phone.
4. Press **Done**. **Your authenticator** now says **Enabled**, with how many backup codes you have left.

6. WHAT YOUR TEAM SEES

1. The next time each person signs in, after their password, they see a square code to scan.
2. They scan it with their authenticator app, type the code under **Verification Code**, and press **Verify & enable**.
3. They save their backup codes, tick **I've saved my backup codes**, and press **Continue to workspace**.

Tip. Tell your team before their next sign-in, so they have the app ready.

7. SIGNING IN EACH DAY

1. After the password, open the app and type the code under **Authenticator Code**. Press **Verify**.
2. On your own work computer, leave **Remember this computer** ticked. You won't be asked for a code on it again for 30 days.
3. Untick it on a shared or public computer.

Tip. Some important actions, like sending a prescription, ask for a fresh code even on a remembered computer.

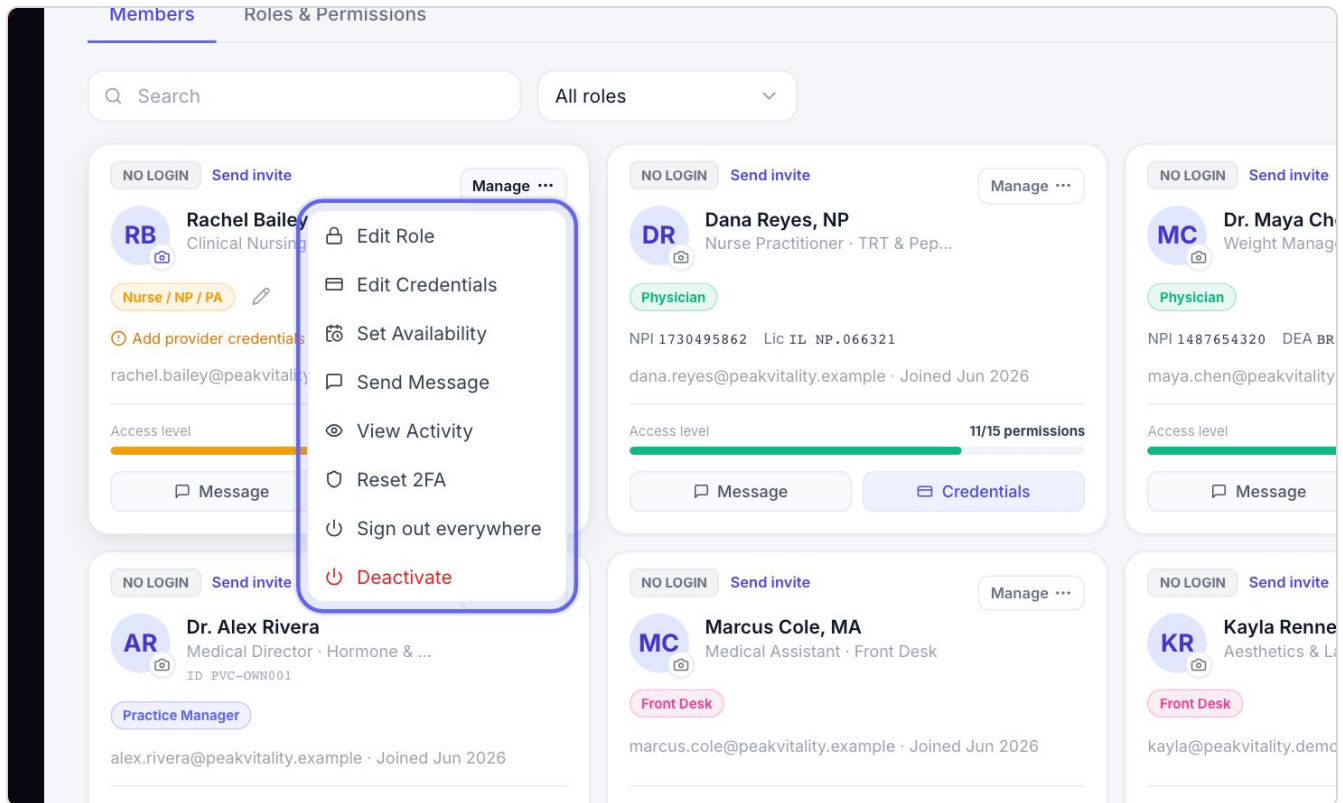
8. IF YOU LOSE YOUR PHONE

1. On the code screen, press **Lost your device? Use a backup code**.
2. Type one of your backup codes and press **Verify**.
3. Once you're in, set up your authenticator on your new phone.
4. Running low on codes? Press **Regenerate codes** under **Your authenticator** for a fresh set, and save them again.

9. RESET IT FOR SOMEONE ON YOUR TEAM

1. If someone has lost both their phone and their backup codes, go to **Team**.
2. Press **Manage** on their row, then **Reset 2FA**. You may be asked for your own code first.

3. They set it up again the next time they sign in.



Team → Manage: Reset 2FA is in this menu.

10. MORE SIGN-IN PROTECTION (OPTIONAL)

1. On the same **Security** page, set the **Session Timeout**: how long an idle computer stays signed in.
2. Set **Lock After N Failures** and the **Lockout Duration**. Wrong codes count the same as wrong passwords.
3. Add your office's **Trusted IP Ranges** to flag sign-ins from anywhere else.

Peak Vitality
Clinic
Growth Plan

Notifications 9+

Dashboard

PATIENTS

Patients

Care Plan

Intake Engine 5

Consents

Appointments

My Schedule

Labs

Treatment Plans

Clinical Notes

PROTOCOLS

Protocols

E-Prescriptions

Refills

TEAM

Dr. Alex Rivera
Owner / Director

Session Timeout

60 minutes

Auto-logout after inactivity

Lock After N Failures

5 attempts

Failed attempts before logout

Lockout Duration

30 minutes

How long the account stays locked

Trusted IP Ranges

CIDR notation (e.g. 203.0.113.0/24), one per line or comma-separated. Sign-ins from outside these ranges are flagged in the security audit trail. To BLOCK a role outright, tick it below.

Office-only roles

Add at least one trusted range above first — with no ranges set, nothing is enforced.

PhysicianNurseMedical assistantFront desk

These roles can ONLY sign in from the trusted ranges above — a sign-in from anywhere else is refused, not just flagged. Owners and managers are never restricted, so a mistyped range can always be corrected.

Allowed to work remotely (exceptions)

No office-only roles selected — there is nothing to make an exception to yet.

Individuals who may sign in from anywhere even though their role is office-only. Use this for the one nurse the medical director has approved, rather than switching the whole role off.

Password Policy (complexity checked when staff set their password · rotation enforced at login)

Minimum Length

12 characters

Force Rotation Every

90 days

How often staff must change their password

Require uppercase + lowercase

Passwords must mix letter cases

Require a number

Passwords must contain at least one digit

Require a symbol

Passwords must contain at least one special character

Session timeout, logout, and your office’s trusted network addresses.