Two-factor Authentication

Last Modified on 11/10/2026 12:22 pm EST

Two-factor authentication adds a second step when you log in on a device Pipeline doesn't recognize: an email to finish logging in, with a link to click or a code to type.

Introduction

A password is one thing standing between a stranger and every file your office keeps in Pipeline. If it leaks, gets reused somewhere that was breached, or is guessed, that's the whole defense gone. Two-factor authentication puts a second thing in the way.

It's a company-level decision rather than a personal preference. Once your account requires it, it applies across the account, and the flexibility comes from exempting particular people rather than from letting everyone choose for themselves. The other thing to understand before switching it on is that the whole scheme rests on your team's login email working. If someone's Pipeline mail is bouncing or landing in spam, the code doesn't reach them, and what was an email problem becomes a locked door.

Turned on, it means a leaked or reused password isn't enough on its own. It also gives you an early warning: if someone receives a code they didn't ask for, somebody else knew their password. And when a user does get stuck at the code screen, they aren't in trouble and nothing is broken. There's a way back in, and support can walk you through it.

How It Works

2FA sits on top of the normal login: password first, then a fresh code from your email.

A Code Sent to Your Email

The second factor is a one-time security code Pipeline emails to your login email address. Codes are email-only — there's no text-message or authenticator-app option.

Turned On for the Whole Company

2FA is an account-wide setting a master admin switches on. Once it's on, it applies to everyone who isn't specifically opted out.

Who Can Opt Out

Even while 2FA is required company-wide, a master admin can opt themselves out, or opt out any individual user (other than another master admin).

Remember a Device for 30 Days

After entering a valid code, you can have Pipeline remember that device for 30 days, so you sign in on it without a code for that window.

A Daily Code Limit

Pipeline sends up to 6 security-code emails per user in any 24-hour period. The limit resets on its own once the window passes, and it can't be raised.

Require Company-wide Two-factor Authentication

Turn 2FA on for everyone from your account's Feature Settings.

Who Can Do This: Master admins.

To require company-wide Two-factor Authentication:

1. Click [Gear] in the upper-right corner, then [Admin / Settings].
2. Scroll down to the **Feature Settings** section.
3. Check [Require two-factor authentication].
4. Click [Save Settings].

From now on, every user who isn't opted out gets an email to finish logging in whenever they log in on a device Pipeline doesn't recognize.

Opt an Individual User Out of Two-factor Authentication

Exempt a single user from the requirement from their profile.

Who Can Do This: Master admins, for any user except another master admin.

To opt an individual user out of Two-factor Authentication:

1. Click the [Gear], then [Admin / Settings].
2. Select [Manage Users] from the People section of the left menu.
3. Click the user's name to open *Edit User*.
4. Check [Opt-out of two-factor authentication].
5. Click [Update User].

That user can now log in without entering a security code, even though 2FA stays required for everyone else.

Opt Yourself Out of Two-factor Authentication

Exempt your own login from the requirement in My Info.

Who Can Do This: Master admins.

To opt yourself out of Two-factor Authentication:

1. Click [Gear] in the upper-right corner, then [My Info].

2. Check [Opt-out of two-factor authentication].
3. Click [Save Settings].

You'll log in with just your email and password from now on, while 2FA stays on for everyone who isn't opted out.

Log In Using Two-factor Authentication

When your company requires 2FA, add a code from your email to finish signing in.

Who Can Do This: Anyone whose company requires 2FA and isn't opted out.

To log in using Two-factor Authentication:

1. Log in at the Pipeline login page with your email address and password as usual.
2. Pipeline emails a security code to your login email address.
3. Open that email and either click the link at the bottom to continue, or return to Pipeline and type in the code.
4. Optionally, check [Remember this device for 30 days] to skip the code on this device for the next 30 days.
5. Click [Continue].

You'll land on the *Home* page.

Frequently Asked Questions

How do I turn on two-factor authentication?

A master admin turns it on company-wide. Go to [Admin / Settings], check [Require two-factor authentication] under Feature Settings, and click [Save Settings]. It's an account-wide setting, not a per-user toggle.

Can I get my security code by text message or an authenticator app?

No — codes are email-only. Every security code is sent to your Pipeline login email address; there's no SMS or authenticator-app option.

Can I turn two-factor authentication off for just one person?

Yes. A master admin can opt any individual user out from that user's profile, even while 2FA stays required for everyone else. Master admins can also opt themselves out in My Info.

Does "remember this device" turn two-factor authentication off?

No. It just skips the code on that one device for 30 days. 2FA stays on everywhere else, and the code returns on that device once the 30 days pass.

Why didn't my security code email arrive?

Almost always your email is blocking it. Check your spam folder first. If a Pipeline email was ever marked as spam, your address can land on a block list that stops delivery — email help@paperlesspipeline.com and we can clear it. If it still won't arrive, your email provider is blocking us and your IT team needs to allow our messages.

I'm locked out after too many code requests — can you reset it?

The daily limit can't be reset. Pipeline sends up to 6 code emails per user every 24 hours. The fix is for a master admin to temporarily opt that user out of 2FA so they can log in, then turn it back on — or wait for the 24-hour window to reset.