Account Settings

Account Settings

This is the page where you change your password, set up a recovery email, pick your timezone, and turn two-factor authentication on or off.

The short version

Account Settings is the home for the things that protect your account and shape how the portal works for you. Most people visit it once when they first sign in — to enable 2FA, set a recovery email, and pick a timezone — and rarely again after that.

There are up to four cards on this page:

- **Change Password** — pick a new password for your account (if your password is managed here).
- **Two-Factor Authentication** — turn on the second sign-in check (a code from an app on your phone, a security key, or a Duo push) so that someone who knows your password still can't sign in without your second factor.
- **Recovery Email** — set a backup email address you can use to reset your password if you ever forget it.
- **Timezone** — tell the system which timezone you're in so that times in the portal and in your vacation auto-reply make sense to you.

Some of these only appear under certain conditions. For example, if your password is handled by your company's main login system, the **Change Password** card is replaced with a short note telling you so. The rest of this page explains each card in turn.

Changing your password

If you see a **Change Password** card with three fields and a Change Password button, your password is managed by Hermes. To change it:

1. Type your current password into the **Existing Password** field.
2. Type your new password into the **New Password** field. It must be between **8 and 64 characters** long.
3. Leave **Check against haveibeenpwned.com** set to **YES** unless you have a specific reason not to. (It quickly checks whether your proposed new password has shown up in a known public data breach. If it has, you'll be asked to pick a different one. The check uses an anonymized fingerprint of your password and does not send the actual password anywhere.)
4. Click **Change Password**.

You can click the small eye icon next to either password field to make the text visible while you type, which is useful when you want to be sure you didn't fat-finger it.

Once the password is changed successfully, you'll see a green confirmation banner. Use the new password the next time you sign in.

"I don't see a Change Password section."

If the card shows a note like "*Your account uses Remote Authentication. Password changes must be made through your organization's directory service*", your password is not stored in Hermes. It's stored in your company's main login system (often Active Directory or a similar directory service). Ask your IT team how to change your password there — once you do, the new password will work for signing in here too.

Your recovery email

The Recovery Email card lets you register a backup email address. This is **not** your main email address on this system — it's an outside address, like a personal Gmail, Yahoo, or Outlook account, that you can get to even if you're locked out of Hermes.

You'd use it if:

- You forget your password and need to reset it yourself, instead of waiting on an administrator.
- You lose access to your two-factor authentication device and need an emergency way back in.

To set one up:

1. Type your outside email address into the **Recovery Email Address** field.
2. Click **Save Recovery Email**.
3. Hermes sends a short verification email to that address. Open it and click the link inside.
4. Come back to this page — the address should now show a green **Verified** badge.

Until you click that link, the address shows a yellow **Not Verified** badge and won't actually work for password recovery. If you didn't get the verification email or accidentally deleted it, click **Resend Verification Email** to send a fresh one. (Check your spam folder too.)

To **change** the recovery email later, type a new address into the update form and submit it — Hermes will send a verification email to the new address, and the old one stays in place until the new one is verified. To **remove** it entirely, scroll to the bottom of the card and click **Remove Recovery Email**.

A couple of important rules:

- The address has to be on an **external** mail provider. You cannot use an address on a domain that Hermes itself handles — that would defeat the purpose, since if you're locked out you'd be locked out of the recovery address too.
- If you don't set a recovery email, that's okay — but if you ever forget your password, you'll have to ask an administrator to reset it for you.

This card only appears if your password is managed by Hermes. If you sign in through your company's directory service, password recovery happens there, not here.

Your timezone

Your timezone affects:

- **Times shown in the portal** (when messages were quarantined, when notifications were sent, and so on).
- **Vacation auto-reply scheduling.** When you set a start and end date for an auto-reply, those times are interpreted as wall-clock times in your timezone. If you say "end at 6:00 PM" and your timezone is `America/New_York`, the auto-reply stops at 6:00 PM Eastern, not 6:00 PM UTC.

To change it, pick a timezone from the dropdown — you can start typing to filter the list, since there are several hundred — and click **Save Timezone**. The current timezone is shown just below the dropdown so you can confirm what it's set to.

One warning about vacation auto-reply

If you already have a vacation auto-reply enabled with a start and end time, changing your timezone will pop up a confirmation box explaining what happens: the wall-clock numbers (like "6:00 PM") stay the same, but they'll now be evaluated in your new timezone. So if you change from `America/New_York` to `Europe/London`, "6:00 PM" suddenly means 6:00 PM London time instead of 6:00 PM New York time — five hours earlier in absolute terms. The dialog lets you confirm or back out.

If you're not sure, leave the timezone alone and adjust the vacation auto-reply dates separately on the Vacation Auto-Reply page.

Two-factor authentication

Two-factor authentication (2FA, sometimes called multi-factor authentication or MFA) is an extra check on top of your password. The idea is simple: when you sign in, you type your password as usual, and then you have to do one more thing — type a code from an app on your phone, tap a notification, or touch a security key. That way, even if someone steals your password, they still can't sign in without your phone or your key.

This is the single most effective thing you can do to protect your account, and it takes about five minutes to set up the first time.

What about my email apps on my phone or laptop?

A quick clarification before we get into setup, because this confuses everyone the first time:

2FA only protects your web sign-in — the User Console and Webmail in your browser. It does **not** affect the email, calendar, or contacts apps on your phone, tablet, or desktop. Those apps use a separate thing called an **app password**, managed under the **My App Passwords** entry in the sidebar. So when you enable 2FA, your phone's Mail app will keep working — it doesn't suddenly start asking you for a code.

If you've never set up an app password, you may need to do that too, but that's a separate page with its own documentation.

What 2FA methods are available

Hermes supports three different second-factor methods. You can pick whichever one you like during the enrollment flow:

- **TOTP** (Time-based One-Time Password) — a six-digit code that refreshes every 30 seconds in an authenticator app on your phone. Works with **Google Authenticator**, **Microsoft Authenticator**, **Authy**, **1Password**, **Bitwarden**, and most other authenticator apps. This is the most common choice and the easiest to start with.
- **WebAuthn** — a hardware security key (like a YubiKey) plugged into your computer's USB port, or a built-in authenticator (Touch ID on a Mac, Windows Hello on Windows, the fingerprint sensor on your laptop). Very secure, but you need either the hardware or a

device that supports a built-in biometric.
- **Duo Push** — a tap-to-approve notification from the Duo Mobile app. Only available if your administrator has Duo Security set up; if it's not listed during enrollment, you don't have it.

If you've never set up 2FA on any service before, **TOTP is the easiest place to start**.

Setting up TOTP step by step

1. Install an authenticator app on your phone if you don't already have one — Google Authenticator, Microsoft Authenticator, and Authy are all free.
2. On this page, in the Two-Factor Authentication card, click **Enable 2FA**. (If you're a mailbox user, the page recommends opening **Webmail** in another browser tab first — you'll need it in a minute to read a verification email.)
3. The system signs you out and sends you back to the sign-in page. Sign in again with your password.
4. After signing in, you're walked through registering a device. Click **Register your first device** and pick **One-Time Password**.
5. A verification email is sent to your mailbox to confirm it's really you. Open it (in your Webmail tab) and click the link inside.
6. A QR code appears on the screen. Open your authenticator app, tap the "+" or "Add account" button, point your phone's camera at the QR code, and the app captures it.
7. The app now starts showing a 6-digit code that changes every 30 seconds. Type the current code into the field on the website and submit.

You're done. From now on, every time you sign in to the portal, after typing your password you'll be asked for the current code from the app.

Backup codes

When you register a TOTP device, the enrollment screen may also offer you a set of one-time **backup codes** — short codes you can use to sign in if you ever lose your phone. **Save these somewhere safe** (a password manager, or printed and stored in a drawer). Each one works exactly once. Without backup codes (or a second registered device, or your recovery email), losing your phone means asking an administrator to reset your 2FA.

"I lost my phone. How do I get back in?"

In order of preference:

1. **Use a backup code** at the 2FA prompt, if you saved any.

2. **Use a second registered device** if you registered more than one (for example, a security key as well as an authenticator app).
3. **Use your recovery email** — if you set one up under the Recovery Email card above, you can use it to start a password reset flow that also resets your 2FA.
4. **Contact an administrator.** They can clear your registered devices so you can enroll a new one. This is the slowest option, which is why setting up backup codes and a recovery email matters.

"Required by your administrator"

If you see a small yellow **Required by your administrator** badge next to your 2FA status, your organization requires 2FA on your account and you can't turn it off from this page. The Disable button is greyed out. If you need to swap out a registered device (for example, you got a new phone and want to re-register TOTP on it), contact your administrator — they can clear your existing device so you can enroll a new one.

If 2FA is required and you haven't enabled it yet, the page shows a yellow **Action required** box with a step-by-step walkthrough. Follow it — the rest of the portal may be locked down to this page and a few others until you finish enrolling.

Frequently asked questions

My password change keeps failing with "The Existing Password you entered is incorrect" — but I'm sure it's right. Double-check for typos using the eye icon to make the text visible. If it really is the right password and it's still failing, your account may be in an odd state — contact an administrator. (If you're certain you've forgotten it, use the **Forgot Password** link on the sign-in page; that uses your recovery email if you set one.)

Can my password contain spaces or special characters? Yes. Any printable character is allowed. The only rule is the length: 8 to 64 characters.

Why does it say "previously appeared in a data breach"? The HIBP check (Have I Been Pwned) compares an anonymized fingerprint of your proposed password against a public database of passwords that have been exposed in past breaches. If it matches, the password is publicly known and attackers have it on their wordlists — even if it's not specifically associated with you. Pick a different one. Random or passphrase-style passwords nearly always pass.

I set up 2FA but my email app on my phone stopped working. 2FA shouldn't affect mail apps — they use app passwords, not your main password. If your mail app stopped working around the same time you enabled 2FA, it's almost certainly that the app was using your main password and now needs an app password instead. Visit **My App Passwords** in the sidebar.

Why does the page tell me to open Webmail in a new tab before enabling 2FA? During 2FA enrollment, Authelia sends a verification email to your mailbox to confirm it's really you. If 2FA isn't set up yet, you're stuck in a chicken-and-egg situation — you can't sign in to Webmail to read the email because 2FA is mid-enrollment. Opening Webmail in a separate tab *before* you click Enable means that tab stays signed in and you can still read the verification email from there.

Do I have to re-do 2FA every time I sign in? You'll be asked for your second factor on each new sign-in, yes. Many browsers and devices give you an option during sign-in to "remember this device" for a period of time, which skips the second factor on that specific device until the remember-me window expires.

The Recovery Email field won't accept my work email. The recovery email has to be on a mail provider that's not handled by this system. The whole point is that it should still work if you're locked out of Hermes. Use a personal Gmail, Yahoo, Outlook, or similar address.

I don't see a Timezone card. Like the Recovery Email card, Timezone only appears if your password is managed by Hermes. If you sign in through your company's directory service, timezone preferences for this portal aren't currently offered — talk to your administrator if dates and times are showing in an inconvenient timezone for you.

Can my administrator see my recovery email or my 2FA devices? Your administrator can see whether you have a recovery email set and whether 2FA is enabled, and they can clear (but not see) your registered 2FA devices. They cannot see your password. They generally do not need to look at this information unless you ask them to help you with account recovery.

Where to next

- **Manage app passwords for your phone, tablet, and desktop email apps** — see *My App Passwords*
- **Turn quarantine notification emails on or off** — see *Notification Settings*
- **Set up a vacation auto-reply** (now that your timezone is correct) — see *Vacation Auto-Reply*

Revision #8
Created 2026-05-31 12:52:44 UTC by Dino Edwards
Updated 2026-06-13 12:29:43 UTC by Dino Edwards