My App Passwords

My App Passwords

This is where you create and manage app passwords for your mailbox — the per-device credentials that mail apps, calendar apps, and contacts apps use to connect to your account.

If someone has just told you to "create an app password" to set up your email on your phone, this page is what they meant. The first few sections below explain what an app password is and why it exists; the rest is the step-by-step for actually using the page.

The short version

An **app password** is a separate password you create for each app or device that connects to your mailbox. It is not your main password. You can have as many app passwords as you want, and you can revoke any one of them without affecting the others.

You use:

- Your **main password** (the one you use to log into the website) when you sign in to the user portal or webmail in your browser.
- An **app password** when you set up the Mail, Calendar, or Contacts app on a phone, tablet, or computer.

This page is where you create, label, and revoke those app passwords. The typical workflow is: click **Create App Password**, type a label that tells you which device it's for ("iPhone", "Thunderbird", "Home laptop"), copy the password the page hands back, and paste it into the app on the device. From then on the device remembers it and you never have to think about it again — until one day you replace the device or lose it, at which point you come back here and click **Revoke** on that row.

This page only exists for mailbox users. If you're a relay-only user (your mail goes through Hermes but isn't stored here), the page will tell you app passwords aren't available for your kind of account, because you have no mailbox to connect to.

Why a separate password from your main one?

Three reasons.

1. You can disable one device without changing the others

Imagine your only password is your main password, and you set it up on your phone, your laptop, and your home computer. Then you lose your phone.

To prevent the lost phone from accessing your email, you would have to **change your main password**, then go back to the laptop and the home computer and re-enter the new password on each. Anything you missed would stop working. And the password would now be different from what you use to log into the website too.

With app passwords:

- You created one called "iPhone" for your phone.
- You created one called "Laptop" for your laptop.
- You created one called "Home" for your home computer.
- You lost your phone — you sign in to the user portal, click **Revoke** next to "iPhone", and that's it.
- Your laptop, your home computer, and your main website login are completely unaffected.

2. Apps cannot do two-factor authentication

When you log into the website, you are sometimes asked for a second factor — a code from an app, or a tap on Duo Push. That extra step keeps your account safer.

Mail apps, calendar apps, and contacts apps cannot ask you for a second factor. They can only send a username and a password, once, and that's it. If you used your main password in those apps, you would be giving them a way around the second factor entirely.

App passwords solve this cleanly: the website still asks for the second factor (because it can), and your apps use a separate, scoped password that has no special powers beyond

mail/calendar/contacts access.

3. App passwords have less power than your main password

Your main password is the key to your whole account. An app password can only be used to access mail, calendar, and contacts. It cannot change your password, change your settings, or access anything else.

So if an app password is somehow stolen, the attacker can read your mail — bad, but not catastrophic. If your main password is stolen, the attacker can do anything you can do.

What an app password looks like

When you create one, the system generates a random string of about 30 characters that looks something like this:

```
xQ7kP2mN9vRtY8wJ3hF6aD1sZ4bC0nL5
```

You will see it **once**, on the screen, right after you create it. You should immediately:

1. Copy it (or scan the QR code the page also shows), and
2. Paste it into the app or device where you want to use it (or save it in a password manager).

After you leave that page, **the system will not show it to you again**. This is intentional — even an administrator cannot retrieve it. The system only stores a one-way scrambled fingerprint of the password, which is enough to check sign-ins but not enough to reveal the password itself. If you lose it before you set up your device, just revoke it and create a new one. There is no penalty for doing this.

You do not need to remember an app password. You will probably never type it manually. The whole point is that you set it once on the device and then forget about it.

What this page shows

There's one button at the top — **Create App Password** — and below it a card called **Active App Passwords** listing every app password that's currently working on your account. The columns are:

Column	What it shows
Label	The name you gave the app password when you created it.
Created	When you created it.
Last Used	When something last successfully signed in with it. Shows **never** if it's been minted but hasn't been used yet (for example, you created it but haven't finished setting up the device).
Action	A red **Revoke** button for that row.

If you have no active app passwords yet, the table is replaced with a short message pointing you at the Create button.

Below the active list, if you've revoked any app passwords in the past, there's a collapsed **Revoked (most recent 50)** card. Click the plus icon in its header to expand it. The revoked list is read-only and is just for your reference — it shows the label, the date it was created, and the date it was revoked.

Creating an app password

1. Click the blue **Create App Password** button near the top of the page. A small dialog opens.
2. In the **Label** field, type a short name for what you're setting up — something like *iPhone*, *Thunderbird*, *Laptop*, or *Outlook on home PC*. The label is for your eyes only; it just helps you remember which row is which when you eventually need to revoke one. (Up to 100 characters.)
3. Click **Create**.
4. The page reloads with a yellow callout at the top headed **Your new app password**. Inside the callout is the password itself — a 30-character random string in a monospace box — and a **Copy** button that puts it on your clipboard. Below the password box there's also a QR code.
5. **Copy the password right now**, or scan the QR code with your phone, and paste the result into the app or device you're setting up. If you're sitting at your laptop minting a password for your phone, the QR code is the easiest path — open your phone's camera or QR scanner, point it at the code, and your phone will offer to copy the text so you can paste it into the Mail app's password field.
6. Once you leave the page or refresh it, the password disappears and **cannot be retrieved** — not by you, not by your administrator.

If you closed the page before copying the password, or you mistyped it into the device and don't know which character was wrong, the fix is simple: revoke that row, create a fresh one, and use the new password instead. There's no penalty for doing this — you can mint and revoke as many as you need.

Revoking an app password

1. Find the row you want to remove in the **Active App Passwords** table.
2. Click the red **Revoke** button on the right side of that row.
3. A confirmation dialog appears asking "*Revoke [label]?*" with a red warning that the device using this password will be locked out immediately. Click **Revoke** to confirm or **Cancel** to back out.

The revocation takes effect right away. The next time the device tries to fetch mail, send mail, sync calendars, or sync contacts using that app password, it will get an authentication error — usually the device pops up a "password incorrect" prompt or shows a red exclamation point next to the account.

To restore that device's access, you create a fresh app password (using the steps above) and enter the new password where the device is asking. There's no way to undo a revocation — but creating a replacement only takes a minute.

The revoked row moves from the Active list to the **Revoked (most recent 50)** list below, where it stays as a record of what was revoked when.

What an app password is good for

Each app password lets a device sign in for:

- **Mail** (IMAP for reading mail, SMTP for sending mail)
- **Calendars** (CalDAV)
- **Contacts** (CardDAV)

So one app password for your phone is enough to set up the Mail app, the Calendar app, and the Contacts app on that phone — you don't need a separate password for each. The same is true for any other device that handles mail, calendars, and contacts together.

App passwords cannot be used to log into the user portal, change your account settings, or do anything else outside of mail/calendars/contacts. That limited scope is deliberate.

How many app passwords should you have?

One per device or app, with a label that tells you which is which. For example:

```
iPhone               (Mail app on your iPhone)
iPad                 (Mail and Calendar on your iPad)
Thunderbird          (the desktop mail client on your laptop)
Outlook on home PC   (the mail client on your personal computer)
Backup tool          (an automated mail backup tool, if you have one)
```

You can also use one app password for multiple things on the same device — for example, a single "iPhone" app password can be used by Mail, Calendar, and Contacts on that one phone — but the cleanest practice is one per device.

When to create or revoke one

Create a new app password when:

- You're setting up a new device or app for the first time (you got a new phone)
- You're replacing an existing device (create a new app password for the new phone, set it up, then revoke the old phone's app password)
- You forgot to copy one when you created it — just revoke that row and create a fresh one

Revoke an app password when:

- You lost a device — revoke that device's app password immediately. The lost device is then locked out, and your main password and other devices are unaffected.
- You stopped using a device or app — revoke its app password to keep your account tidy.
- You suspect an app password was stolen — revoke it. Even if you are not sure, revoking and creating a new one takes about a minute.

What about your main password?

You still have one, and you still use it for the website (and webmail, calendar, and contacts when you access them through the website). You should keep it strong, keep it private, and change it if you ever suspect it has been compromised.

What changes is that **your main password no longer has to live on every device you own**. It only ever leaves your head when you type it into the website. Your devices have their own credentials, and those credentials are limited to the apps they were created for.

Common scenarios

Setting up your first device. Click **Create App Password**, label it for the device (for example, *iPhone*), copy the password the page shows you, and paste it into the device's mail/calendar/contacts settings as the password. Your normal email address is the username. If you're following one of the mobile setup wizards under *Set Up Your Devices*, those wizards take care of generating and applying the app password for you and you may not need to visit this page at all.

Replacing a device. Create a new app password labelled for the new device (for example, *iPhone (new)*), set up the new device with it, confirm mail, calendar, and contacts all work, and only then revoke the old device's row.

Lost device. Open this page, find that device's row, click **Revoke**, and confirm. The lost device is locked out within seconds. Your other devices, your main password, and your webmail sign-in are completely unaffected.

Lost the password before you set up the device. Revoke the row you just created and create a fresh one. The label can be the same as before — it doesn't have to be unique.

You stopped using an app or device. Revoke its row. There's no harm in leaving old app passwords active, but keeping the list tidy makes it obvious which ones are real and which would never legitimately sign in.

Frequently asked questions

My phone is asking for a password I don't have. What do I enter? Sign in to the user portal, come to this page, click **Create App Password**, label it for the device you're setting up, copy the password it shows you, and paste it into the phone. That's the password the phone is asking for.

Why did the page only show the password once? Because the system never stores the actual password — only a one-way scrambled fingerprint of it. That fingerprint is enough to check whether the password a device sends in is correct, but it's not enough to reconstruct the password itself. The plaintext exists for a few seconds in your browser at creation time, and then it's gone. This is intentional and matches how every reasonable system handles passwords.

I copied the password but my device says it's wrong. What happened? The most common cause is a copy-paste mistake — a stray space, a missed character, or the device accidentally autocorrecting part of it. Try copying it again carefully. If it still doesn't work and you're already past the "shown once" screen, revoke the row and create a fresh one. The new password will work cleanly.

What does the label do? Nothing technical. It's a name you give the app password so that later, when you need to revoke one, you can tell at a glance which row is which. Hermes does not check the label against the device or care what's in it. Pick anything meaningful to you.

Can I rename a label later? No. Labels are set at creation and don't change. If a label became wrong over time (say you labelled it *iPhone* and you now use it on your iPad), the easiest fix is to revoke and re-create with the new label.

The Last Used column says "never" for a password I'm definitely using. "Last Used" is updated by the system when a sign-in succeeds. If your device is set up to check mail only on demand, or if it hasn't connected in a while, the column may lag. Give it a few minutes after the device next fetches mail and reload the page.

Can I share an app password with someone else? Don't. App passwords are device-scoped, but they are still credentials to your mailbox. If you need someone else to access shared content (a shared inbox, a shared calendar), the administrator can grant that access without sharing any password.

Will revoking an app password log me out of the user portal? No. The user portal uses your main password (and 2FA, if enabled), not an app password. App passwords are only used by mail, calendar, and contacts apps.

Does the QR code contain anything besides the password? No. It encodes the 30-character password and nothing else — no URLs, no account information, no metadata. Scanning it just puts the password on your phone's clipboard so you can paste it into the Mail app.

Where to next

- **Set Up Your Devices** — step-by-step mobile setup wizards that generate and apply an app password for you. Often the easiest path for phones and tablets.
- **Account Settings** — change your main password, set a recovery email, manage two-factor authentication.

Revision #25
Created 2026-05-31 12:52:46 UTC by Dino Edwards
Updated 2026-06-20 13:32:45 UTC by Dino Edwards