

Two-factor authentication and security keys

What this is about

Your panel account controls your servers, worlds and backups, so it's worth protecting with more than a password. Two options are available:

- **Two-factor authentication (2FA)**: after your password, you enter a 6-digit code from an app on your phone.
- **Security keys / passkeys**: sign in with your fingerprint, face, phone or a hardware key, with no password needed.

You can use either one, or both.

Setting up two-factor authentication

You'll need an authenticator app on your phone, such as Google Authenticator, Microsoft Authenticator, Authy or 2FAS.

1. Click your name (bottom-left) to open **Account**.
2. In the **Two-Factor Authentication** card, click **Setup Two-Factor**.
3. Scan the **QR code** with your app (or type in the code shown under it).
4. Enter the **6-digit code** from your app and your **password**, then click **Enable**.

Setup Two-Factor Authentication

Help protect your account from unauthorized access.
You'll be prompted for a verification code each time you sign in.



Scan the QR code above using the two-factor authentication app of your choice. Then, enter the 6-digit code generated into the field below.

Authentication Code *

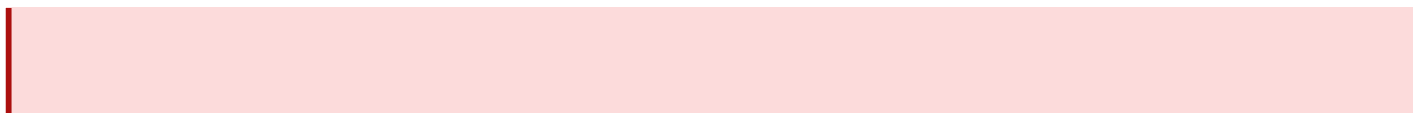
Password *

Enable

Close

Save your recovery codes!

You'll now be shown **10 recovery codes**. **Copy them and keep them somewhere safe:** a password manager, or printed out. Each code works once and lets you in if you lose your phone.



You will only see these codes once. If you lose your phone *and* your recovery codes, you'll need to contact support to get back in.

Signing in with 2FA

After your password, enter the 6-digit code from your app and click **Verify Code**. Lost your phone? Click **Use Recovery Code** and enter one of your saved codes.

"Invalid code"? Codes depend on your phone's clock. Make sure its time is set automatically. The panel also warns you if your computer's clock is off.

Turning 2FA off (or moving to a new phone)

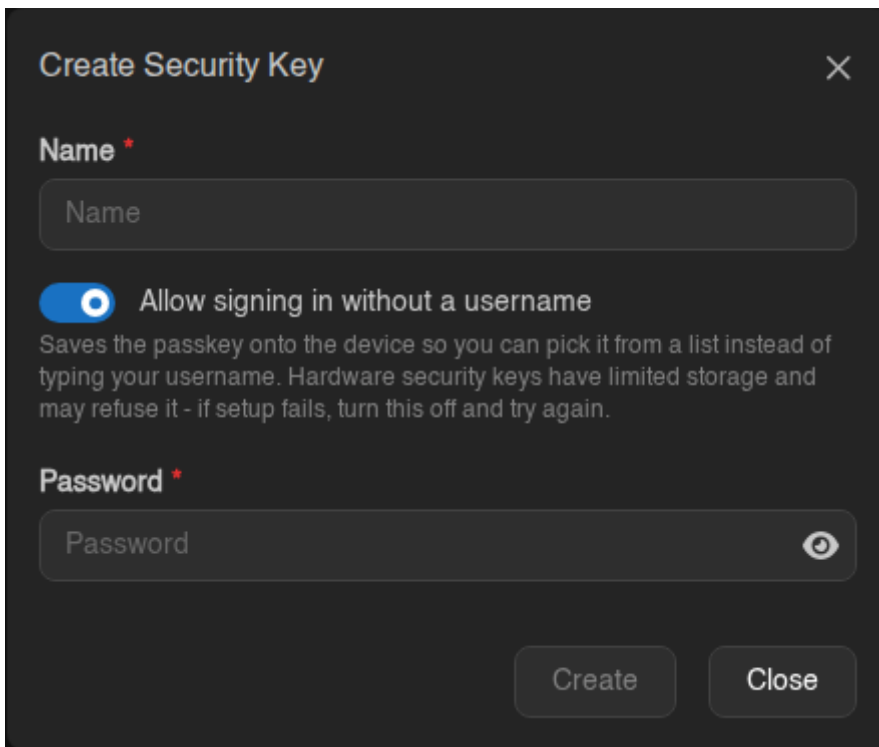
Click **Disable Two-Factor**, enter a code from your app (or a recovery code) and your password, then click **Disable**. To move to a new phone, disable it and set it up again on the new one.

Security keys and passkeys

A **passkey** lets you sign in with your device's fingerprint reader, face unlock, PIN, or a hardware key like a YubiKey. You don't type a password, and it can't be phished.

Adding one

1. Go to **Account** → **Security Keys** and click **Create**.
2. Give it a **Name** (e.g. "My laptop") and enter your password.
3. Leave **Allow signing in without a username** on, so you can sign in with one click.
4. Click **Create** and follow your browser or phone's prompt.



Create Security Key

Name *

Name

☒ Allow signing in without a username

Saves the passkey onto the device so you can pick it from a list instead of typing your username. Hardware security keys have limited storage and may refuse it - if setup fails, turn this off and try again.

Password *

Password

Create Close

Using an older hardware key and setup fails? Turn **Allow signing in without a username** off and try again. Some keys have limited storage.

Signing in with a passkey

On the login page, click **Sign in with a Passkey** and follow the prompt. Or type your username and choose **Use Passkey**.

Turning off password login (optional)

Once you have a passkey, you can stop your password working entirely: in the **Password Login** card on the Account page, click **Disable**.

This also stops your password working for **SFTP**, so you'd need an [SSH key](#) for that. Make sure your passkey works before turning this off.

Lost access?

- **Lost your 2FA phone:** sign in with a recovery code, then set up 2FA again.
- **No phone and no recovery codes:** open a support ticket from your [billing account](#). We'll verify it's you before removing 2FA.

Revision #5

Created 2026-10-23 15:18:48 UTC by Brandon F

Updated 2026-10-23 15:30:44 UTC by Brandon F