Help & User Guide

Version 2.55-demo

This guide is written in both languages — English (from page 1) · Român■ (de la pagina 7).

English

ThorStorage is a secure backup-storage server with a web admin. You create FTP accounts — each with its own private folder — and connect over encrypted FTPS to upload and download backups. It also plays videos in the browser and casts them to a Chromecast. There are two roles: an **admin** manages the whole server; a **tenant** manages only their own private space and cannot see other tenants.

Why ThorStorage?

- Your own private backup server — your data stays on your hardware, not a third-party cloud.
- Encrypted end to end — FTPS for transfers, HTTPS for the web admin.
- Simple for everyone — a clean web admin, no command line needed.
- Multi-tenant — give each client or department its own isolated space and quota.
- More than backups — stream and cast your videos straight from storage.

Signing in

First sign-in with the default admin account requires setting a new password, then accepting the Terms & Privacy agreement (everyone re-accepts if the terms change).

Forgot your password? Use the link on the sign-in page to get a reset email (when mail is configured). Repeated wrong attempts are temporarily blocked. “Remember me” keeps you signed in on that device; switch language any time with EN / RO.

Dashboard

Your home screen shows a storage overview (space used vs available and the number of FTP accounts), the list of FTP accounts with their folder and size, your folders, and recent sign-ins.

FTP backup accounts

Add an FTP account and its private folder in one step (use **Generate** for a strong 12-character password). Each account is locked to its own folder and can use FTP only — no shell or SSH. Backup tools log in over FTPS. A tenant can create up to 100 accounts, and names the system already uses (root, ftp, www-data, thorjob and the like) are reserved.

When you create an account you can point it at any folder from the list — including a **subfolder** of an existing one, not just a top-level folder. Use **Edit** on an account’s row to change its password or move it to a different working folder later; moving only re-points where the account opens — it never moves files already on disk (they stay where they are, visible to you in Files, and you can re-point the account back if you want them).

Files, folders & uploading

Open **Files** to browse. Create folders (spaces allowed), download any file, and delete files or folders (recursive, always confirmed). An FTP account's main folder is protected: it cannot be deleted from Files, only by deleting the account it belongs to — and even then the folder and its data are kept unless you separately confirm that they should be erased too.

Use the **search box** at the top of a folder to find a file by name anywhere beneath it — each result shows the folder it lives in, so you can jump straight there. Click any column header to **sort** the list (by name, size, or date — sizes and dates sort correctly, not alphabetically); the FTP-accounts, Users and Vault lists also have a quick filter box that hides non-matching rows as you type.

To work on several files at once, tick their checkboxes — or use **Select all** above the list, which becomes **Unselect all** once everything is ticked. Folders have no checkbox: a selection is always a set of files. Then use **Move selected…** to move them into another folder you control, or **Delete selected** to remove them all after one confirmation.

Upload any way you like: drag & drop files or a whole folder (subfolders are recreated), "upload a folder", drop an image from another web page, or paste from the clipboard. Each file shows a progress bar with Cancel; uploads never overwrite; everything is auto-owned by the folder's FTP account.

Temporary download links

On any file, click **Link** to create a shareable, expiring download link. Anyone with the link can download that one file — no sign-in needed — until it expires, and each link is unique every time you generate one.

An admin sets how long links stay valid (in hours) under **Settings › Download links**. The setting applies to every link, including ones already handed out.

Temporary upload links

On any folder you control in **Files**, click **Upload link** to create a temporary link that lets someone **outside** upload files into that folder — with no sign-in. You choose how long it stays valid (up to 48 hours; the default comes from Settings) and can optionally cap the total size and the number of files. You can also set an **optional password** the person must enter before uploading — set, change, generate or remove it any time, and share it separately from the link (it never travels in the link itself).

Share the link with whoever should send you files: they open it and drag & drop, no account needed. Dangerous file types are refused, and everything they upload lands owned by the folder's FTP account.

Under the **Upload links** menu you see all your links, and for each one the files that were uploaded together with the source IP of each upload. A link stops working the moment it expires, you revoke it, or it reaches a limit; you can also delete links (one, several, or all). These links are reachable from outside the firewall over the public link port, which an admin enables under Settings.

Vault — encrypted files

The **Vault** is a private, encrypted folder in your own space, used from the web only (never over FTP). Files you put there are encrypted on the server with a passphrase you choose — nobody, not even the server operator, can read them without it (zero-knowledge). What you keep there counts toward your storage quota, together with your FTP folders.

Create it once with a strong passphrase (min. 12 characters; press **Generate** to make one) and store that key somewhere safe. Unlock it to upload (drag & drop, whole folders, paste or a dropped link), download or delete; Lock it when done. You can change the passphrase — the whole vault is re-encrypted safely.

Warning: the passphrase is the ONLY key. If you lose it the files CANNOT be recovered — you can only Reset the vault, which permanently deletes everything in it.

Password Manager

ThorStorage includes a **zero-knowledge password manager**: a browser extension (Chrome and Firefox) that keeps your logins encrypted and syncs them to ThorStorage. The server only ever stores ciphertext.

On the **Passwords** page you set up a **dedicated access username and password** — kept separate from your ThorStorage login on purpose, so a browser compromise can't reach your account. Download the extension there (or scan the QR), enter that access, and it walks you through saving a **recovery key** and choosing a **master password** that encrypts everything in the browser and never leaves it.

It then offers to save logins as you sign in, fills them on your next visit, and can optionally turn off the browser's built-in manager so it becomes your default. Enrolled browsers are listed and revocable.

Warning: the master password and recovery key never leave the browser and are the ONLY keys — lose both and the saved passwords cannot be recovered.

Video player & casting

Click **Play** to open the player (it does not autoplay). Choose the aspect (16:9 default; also Fit, Zoom, Stretch, 4:3), turn subtitles on/off or switch language, and — when casting — switch the audio track. Downloading from the player is disabled.

Press **Cast** and pick your Chromecast: a short branded intro plays, then your video. The TV shows only “Playing from ThorStorage”, never the file name.

Streaming — URL streams (admin)

When an admin turns on **URL streaming** (Settings › URL streaming), a **Streaming** menu appears for adding named external stream links — MP4, HLS (.m3u8) or MPEG-TS (.ts), such as IPTV channels.

Play a link in the browser or cast it to a Chromecast on your network. The server fetches the stream and relays it, so the source URL is never exposed to the browser or the TV, and only a token issued by the app can start it. Click a name to edit it, **Test** to check the source is reachable, or **Delete**.

Scheduler — scheduled scripts

When an admin enables the **Scheduler** (Settings › Scheduler), a **Scheduler** menu appears. Create a job by pasting a script or picking a script file from your storage, choose an output folder, and set when it runs — daily, weekly, monthly, once, or a custom cron expression.

Every run is **sandboxed**: the job runs under a restricted account with CPU, memory, process and run-time limits; it can read only its own script, write only to the output folder and a temporary folder, and has no network access unless you allow it. It can never see the application's files or another user's data. Your script receives OUTPUT_DIR, TEMP_DIR, STATE_DIR, JOB_NAME and RUN_TIME as environment variables — OUTPUT_DIR is published after the run and TEMP_DIR is wiped, while **STATE_DIR** is a small folder that PERSISTS between runs (keep an index or a cursor there, e.g. for an incremental sync).

Network access is decided per job — the **Allow network access** box, off by default — and an administrator can block it for every script at once from Settings › Scheduler (also off by default, so users normally keep deciding for their own jobs). A job that is allowed out still cannot reach this server itself: loopback, link-local addresses and the box's own addresses are refused.

Each run is logged with its output, errors, exit code and duration, so a failure, a timeout or a memory-limit kill is easy to tell apart; only the most recent runs are kept per job (five by default, an admin can set 1–200). Tick **Email me if a run fails** on a job to be emailed the details (job name, result, and the error) at your account's address whenever a run fails — this needs the server's email (SMTP) to be configured.

At most two jobs run at the same time. If more fall due at once — say ten backups all set for 02:00 — the extras wait in a queue and start a couple at a time as slots free, so none are dropped and each runs exactly once. Scripts can import ready libraries with nothing to install: SSH/SFTP (paramiko), HTTP (requests), MySQL (pymysql) and PostgreSQL (psycopg2), plus **FTP and FTPS** from Python's own `ftplib` (FTP and FTP_TLS). After the server reboots nothing runs for 5 minutes, which gives you time to switch off a job that is overloading the machine; an admin can also suspend all job execution at any time from Settings.

Tenants (admin)

Under **Users**, create a tenant (a web login with its own private space) with an email and a storage quota. Each row lets you open, edit, or delete the tenant.

Editing a tenant · quotas & FTP suspension

On a tenant's **Edit** page, change its recovery email or quota, email a password-reset link or set a new password, and re-enable FTP. The username can't be changed.

Each tenant can have a storage quota in GB (0 = unlimited; new tenants default to 10 GB). What counts toward it is everything the tenant keeps on the box: their FTP folders and their Vault together. When a tenant goes over quota, web uploads are refused and its FTP logins are suspended automatically, then restored automatically once usage drops back under the limit. The tenant is emailed on both changes — the suspension message says plainly that backups sent over FTP will fail to log in until they free some space.

Reports (admin)

Storage and sign-in statistics: capacity and usage, each user's last sign-in with IP and device, and recent sign-in history. Export to CSV or PDF.

System resources (admin)

The Reports page also shows live server health: memory (RAM) used vs. total, the number of CPU cores with per-core busy percentages, and the load average — so you can see at a glance how hard the box is working.

Logs (admin)

A rotating diagnostic log of streaming, media access and errors. View it in the app or purge it; it rotates automatically at 100 MB.

Settings

Change your password and contact email. Admins can also configure the mail (SMTP) account used for password-reset emails, the Chromecast receiver App ID, the Scheduler, whether FTP encryption is required, the domain & HTTPS certificate, the server time (timezone + NTP), the access-control firewall and IPv6, and how long temporary download links stay valid — each covered below.

Automatic sign-out (admin): sign every account out of the web panel after a period of inactivity (30 minutes by default). It applies to everyone; while it is on, “Keep me signed in” is hidden and ignored so a session can never outlive the timeout. It is on by default — turning it off is flagged as a security risk. A correct password always signs you in, even right after too many wrong attempts, so nobody can be locked out of the panel by someone guessing their password.

Time & date — timezone and NTP (admin)

Set the server timezone (pick continent then city) and the time servers (NTP) the box syncs its clock from. Each time server is verified to actually respond before it is saved, and a status line shows whether the clock is in sync. Correct time keeps logs, certificates and reports accurate. If the clock is far out, use **Sync clock now** — the background time service only nudges small differences and would never close a large gap on its own.

Network — IP address (admin)

Under **Settings** you set the server's IP: a fixed (static) address or automatic (DHCP). After you apply, you confirm from the new address within 90 seconds or it reverts automatically — so a wrong setting can’t lock you out.

When you access the exact IP being changed you’re taken to the new address automatically; through a domain or behind NAT it confirms on its own if that address stays reachable, and reminds you to point your router’s port-forward at the new IP first (or confirm from inside the LAN).

Firewall & access control (admin)

Restrict which source addresses may reach the machine: turn on access filtering and list the allowed IPs or ranges (CIDR). Your current address is always allowed, so you can’t lock yourself out — and after you apply new rules the page confirms you’re still connected; if it can’t, the previous rules are restored automatically after a minute.

IPv4 and IPv6 are shown separately, read from the rules the machine actually has loaded. IPv6 is off unless you switch it on in the same card — while it is off the appliance has no IPv6 address at all. The list takes both IPv4 and IPv6 entries and applies each to its own family. While a Let’s Encrypt certificate is being issued or renewed, port 80 is briefly open for the validation and firewall changes are refused for that minute.

Automatic updates (admin)

The server checks daily for a new, digitally-signed release. When one is available you can apply it with one click — a safe self-update that swaps the app and restarts, keeping all your data, accounts and settings. Every update is verified by signature and checksum before it is installed, and a background watchdog rolls back automatically if a new version fails to start.

Domain & HTTPS certificate (Let’s Encrypt)

Enter your domain and email and request a free Let’s Encrypt certificate — it secures both the web admin (HTTPS) and FTP (FTPS) and renews automatically. Point the domain’s DNS at this server before requesting.

Install on your phone (as an app)

Android (Chrome): open the app’s HTTPS address, tap the ■ menu, choose “Install app” / “Add to Home screen”, and launch it from the new icon.

iPhone / iPad (Safari): open the HTTPS address in Safari, tap the Share button, choose “Add to Home Screen”, then Add. It runs full-screen like a native app.

Connecting over FTPS

Use an FTP account’s credentials with a client that supports **explicit FTP over TLS** (FTPS) in **passive** mode. Control port **21**, passive data ports **40000–40100** — open these in your firewall.

FileZilla / WinSCP: Host, Port 21, Protocol FTP, Encryption “Require explicit FTP over TLS”, Logon Type Normal, then the account user + password; Transfer mode Passive.

lftp: `lftp -u <user> ftps://<host>:21`

Security

FTP is encrypted by default — FTPS is required and unencrypted FTP logins are refused. An admin can deliberately allow plaintext FTP under **Settings › FTP encryption** for a client that cannot do FTPS; passwords and files then travel in the clear, so it is a last resort.

FTP accounts have no shell and are locked to their own folder. The web admin is served over HTTPS, with sign-in throttling, CSRF protection and per-tenant isolation.

Român■

ThorStorage este un server sigur de stocare pentru backup, cu administrare web. Creezi conturi FTP — fiecare cu folderul lui privat — ■i te conectezi prin FTPS criptat pentru a înc■rca ■i desc■rca backupuri. Red■ ■i videoclipuri în browser ■i le transmite (cast) c■tre un Chromecast. Exist■ dou■ roluri: un **admin** administreaz■ întreg serverul; un **chiria■** administreaz■ doar spa■iul lui privat ■i nu vede al■i chiria■i.

De ce ThorStorage?

- Propriul t■u server de backup — datele r■mân pe hardware-ul t■u, nu într-un cloud ter■.
- Criptat cap la cap — FTPS pentru transferuri, HTTPS pentru administrarea web.
- Simplu pentru oricine — o interfa■■ web clar■, f■r■ linie de comand■.
- Multi-tenant — fiecare client sau departament are spa■iu izolat ■i cot■ proprie.
- Mai mult decât backup — redai ■i transmi■i (cast) videoclipuri direct din stocare.

Autentificare

Prima autentificare cu contul de admin implicit cere setarea unei parole noi, apoi acceptarea Termenilor ■i a Politicii de confiden■ialitate (to■i reaccept■ dac■ termenii se schimb■).

Ai uitat parola? Folose■te linkul din pagina de autentificare pentru un email de resetare (când e configurat mailul). Încerc■rile gre■ite repetate sunt blocate temporar. „■ine-m■ minte” te p■streaz■ autentificat pe acel dispozitiv; schimbi limba oricând cu EN / RO.

Panou principal

Ecranul principal arat■ o privire de ansamblu a stoc■rii (spa■iu folosit vs. disponibil ■i num■rul de conturi FTP), lista conturilor FTP cu folderul ■i dimensiunea lor, folderele tale ■i autentific■rile recente.

Conturi FTP de backup

Adaugi un cont FTP ■i folderul lui privat într-un singur pas (folose■te **Genereaz■** pentru o parol■ puternic■ de 12 caractere). Fiecare cont e blocat în propriul folder ■i poate folosi doar FTP — f■r■ shell sau SSH. Uneltele de backup se conecteaz■ prin FTPS. Un chiria■ poate crea pân■ la 100 de conturi, iar numele deja folosite de sistem (root, ftp, www-data, thorjob ■i altele asemenea) sunt rezervate.

La creare po■i îndrepta contul spre orice folder din list■ — inclusiv un **subfolder** al unuia existent, nu doar un folder de nivel principal. Folose■te **Editeaz■** pe rândul unui cont ca s■-i schimbi ulterior parola sau s■-l mu■i în alt folder de lucru; mutarea doar schimb■ unde se deschide contul — **nu** mut■ datele deja aflate pe disc (r■mân unde sunt, vizibile în Fi■iere, iar contul poate fi îndreptat înapoi spre ele oricând).

Fi■iere, foldere ■i înc■rcare

Deschide **Fi■iere** pentru a naviga. Creezi foldere (spa■iile sunt permise), descarci orice fi■ier ■i ■tergi fi■iere sau foldere (recursiv, mereu confirmat). Folderul principal al unui cont FTP e protejat: nu poate fi ■ters din Fi■iere, ci doar ■tergând contul c■ruia îi apar■ine — ■i nici atunci folderul ■i datele nu dispar, decât dac■ confirmi separat c■ vrei ■tergerea lor.

Folose■te **caseta de c■utare** din capul unui folder ca s■ g■se■ti un fi■ier dup■ nume oriunde sub el — fiecare rezultat arat■ folderul în care se afl■, ca s■ sari direct acolo. D■ click pe orice antet de coloan■ ca s■ **sortezi** lista (dup■ nume, m■rime sau dat■ — m■rimile ■i datele se sorteaz■ corect, nu alfabetic); listele de conturi FTP, Utilizatori ■i Seif au ■i o caset■ de filtrare rapid■ care ascunde rândurile nepotrivite pe m■sur■ ce tastezi.

Ca s■ lucrezi cu mai multe fi■iere deodat■, bifezi c■su■ele lor — sau folose■ti **Selecteaz■ tot** de deasupra listei, care devine **Deselecteaz■ tot** când e totul bifat. Folderele nu au c■su■■: o selec■ie e mereu un set de fi■iere. Apoi folose■ti **Mut■ selectate…** ca s■ le mu■i în alt folder pe care îl controlezi, sau **■terge selectate** ca s■ le ■tergi pe toate, dup■ o singur■ confirmare.

Încarci cum vrei: tragi ■i plasezi fi■iere sau un folder întreg (subfolderele sunt recreate), „încarc■ un folder”, tragi o imagine din alt■ pagin■ web sau lipe■ti din clipboard. Fiecare fi■ier are o bar■ de progres cu Anulare; înc■rc■rile nu suprascriu niciodat■; totul e atribuit automat contului FTP al folderului.

Linkuri temporare de desc■rcare

La orice fi■ier, ape■i **Link** pentru a crea un link de desc■rcare partajabil, care expir■. Oricine are linkul poate desc■rca acel fi■ier — f■r■ autentificare — pân■ expir■, iar fiecare link e unic de fiecare dat■ când îl generezi.

Un admin stabile■te cât timp r■mân valabile linkurile (în ore) din **Set■ri › Linkuri de desc■rcare**. Setarea se aplic■ tuturor linkurilor, inclusiv celor deja date.

Linkuri temporare de înc■rcare

Pe orice folder pe care îl controlezi în **Fi■iere**, ape■i **Link de înc■rcare** pentru a crea un link temporar prin care o persoan■ din **exterior** poate înc■rca fi■iere în acel folder — f■r■ autentificare. Alegi cât timp e valabil (pân■ la 48 de ore; valoarea implicit■ vine din Set■ri) ■i, op■ional, limitezi dimensiunea total■ ■i num■rul de fi■iere. Po■i seta ■i o **parol■ op■ional■** pe care persoana trebuie s■ o introduc■ înainte de a înc■rca — o po■i seta, schimba, genera sau elimina oricând ■i o trimi■i separat de link (nu c■l■tore■te niciodat■ în link).

Trimite linkul celui care trebuie s■-■i transmit■ fi■iere: îl deschide ■i trage & las■ fi■ierele, f■r■ cont. Tipurile de fi■iere periculoase sunt refuzate, iar tot ce încarc■ r■mâne de■inut de contul FTP al folderului.

În meniul **Linkuri de înc■rcare** vezi toate linkurile tale, iar pentru fiecare fi■ierele înc■rcate împreun■ cu IP-ul surs■ al fiec■rei înc■rc■ri. Un link înceteaz■ s■ func■ioneze imediat ce expir■, îl revoci sau atinge o limit■; po■i ■i ■terge linkuri (unul, mai multe sau toate). Aceste linkuri sunt accesibile din afara firewallului prin portul pentru linkuri publice, pe care un admin îl activeaz■ din Set■ri.

Seif — fi■iere criptate

Seiful e un folder privat, criptat, în propriul t■u spa■iu, folosit doar din web (niciodat■ prin FTP). Fi■ierele puse acolo sunt criptate pe server cu o parol■ aleas■ de tine — nimeni, nici m■car operatorul serverului, nu le poate citi f■r■ ea (zero-knowledge). Ce ■ii acolo intr■ în cota ta de stocare, împreun■ cu folderele FTP.

Îl creezi o dat■ cu o parol■ puternic■ (min. 12 caractere; apas■ **Genereaz■**) ■i p■strezi cheia undeva sigur. Îl deblochezi ca s■ încarci (drag & drop, foldere întregi, paste sau un link tras), s■ descarci sau s■ ■tergi; îl Blochezi când termini. Po■i schimba parola — tot seiful se re-cripteaz■ în siguran■■.

Aten■ie: parola e SINGURA cheie. Dac■ o pierzi, fi■ierele NU pot fi recuperate — po■i doar Reseta seiful, ceea ce ■terge definitiv tot din el.

Manager de parole

ThorStorage include un **manager de parole zero-knowledge**: o extensie de browser (Chrome ■i Firefox) care î■i ■ine parolele criptate ■i le sincronizeaz■ cu ThorStorage. Serverul stocheaz■ doar text cifrat.

În pagina **Parole** î■i setezi un **user ■i o parol■ de acces dedicate** — ■inute inten■ionat separate de login-ul ThorStorage, ca o compromitere a browserului s■ nu ajung■ la cont. Descarci extensia de acolo (sau scanezi QR-ul), introduci acel acces, iar ea te ghideaz■ s■ salvezi o **cheie de recuperare** ■i s■ alegi o **parol■ principal■** care cripteaz■ tot în browser ■i nu îl p■r■se■te niciodat■.

Apoi î■i propune s■ salveze login-urile pe m■sur■ ce te autentifici, le completeaz■ la urm■toarea vizit■ ■i op■ional poate opri managerul nativ al browserului ca s■ devin■ cel implicit. Browserele înrolate sunt listate ■i revocabile.

Aten■ie: parola principal■ ■i cheia de recuperare nu p■r■sesc niciodat■ browserul ■i sunt SINGURELE chei — dac■ le pierzi pe amândou■, parolele salvate nu pot fi recuperate.

Player video ■i cast

Ape■i **Red■** pentru a deschide playerul (nu porne■te automat). Alegi formatul (16:9 implicit; ■i Fit, Zoom, Stretch, 4:3), porne■ti/opre■ti subtitr■rile sau schimbi limba ■i — la cast — schimbi pista audio. Desc■rcarea din player e dezactivat■.

Ape■i **Cast** ■i alegi Chromecast-ul: se red■ un scurt intro cu brand, apoi videoclipul t■u. Televizorul arat■ doar „Playing from ThorStorage”, niciodat■ numele fi■ierului.

Programator — scripturi programate

Când un admin activeaz■ **Programatorul** (Set■ri › Programator), apare meniul **Programator**. Creezi un job lipind un script sau alegând un fi■ier script din stocare, alegi un folder de ie■ire ■i stabile■ti când ruleaz■ — zilnic, s■pt■mânal, lunar, o singur■ dat■ sau cu o expresie cron.

Fiecare rulare este **izolat■**: jobul ruleaz■ sub un cont restric■ionat, cu limite de CPU, memorie, procese ■i timp; poate citi doar propriul script, poate scrie doar în folderul de ie■ire ■i într-unul temporar, ■i nu are acces la re■ea decât dac■ permi■i. Nu poate vedea niciodat■ fi■ierele aplica■iei sau datele altui utilizator. Scriptul prime■te OUTPUT_DIR, TEMP_DIR, STATE_DIR, JOB_NAME ■i RUN_TIME ca variabile de mediu — OUTPUT_DIR se public■ dup■ rulare, iar TEMP_DIR se ■terge, în timp ce **STATE_DIR** e un folder mic care PERSIST■ între rul■ri (■ine acolo un index sau un marcaj, de exemplu pentru o sincronizare incremental■).

Accesul la re■ea se decide pentru fiecare job — caseta **Permite acces la re■ea**, oprit■ implicit — iar un administrator îl poate bloca pentru toate scripturile deodat■ din Set■ri › Programator (tot oprit implicit, deci în mod normal fiecare utilizator decide pentru joburile lui). Un job c■ruia i se permite re■eaua tot nu poate ajunge la acest server: loopback-ul, adresele link-local ■i adresele proprii ale cutiei sunt refuzate.

Fiecare rulare e jurnalizat■ cu ie■irea, erorile, codul de ie■ire ■i durata, deci o eroare, un timp expirat sau o oprire pentru dep■■irea memoriei se disting u■or; se p■streaz■ doar cele mai recente rul■ri pentru fiecare job (cinci implicit, un admin poate seta 1–200). Bifeaz■ **Trimite-mi email dac■ o rulare e■ueaz■** pe un job ca s■ prime■ti detaliile (numele jobului, rezultatul ■i eroarea) la adresa contului t■u ori de câte ori o rulare e■ueaz■ — necesit■ email-ul serverului (SMTP) configurat.

Ruleaz■ cel mult dou■ joburi în acela■i timp. Dac■ mai multe devin scadente deodat■ — de exemplu zece backupuri toate la 02:00 — restul a■teapt■ într-o coad■ ■i pornesc câte dou■ pe m■sur■ ce se elibereaz■ locuri, deci niciunul nu se pierde ■i fiecare ruleaz■ exact o dat■. Scripturile pot importa biblioteci gata de folosit, f■r■ nimic de instalat: SSH/SFTP (paramiko), HTTP (requests), MySQL (pymysql) ■i PostgreSQL (psycopg2), plus **FTP ■i FTPS** din `ftplib` din Python (FTP ■i FTP_TLS). Dup■ repornirea serverului nu ruleaz■ nimic timp de 5 minute, ca s■ ai timp s■ opre■ti un job care supraîncarc■ ma■ina; un admin poate de asemenea suspenda oricând execu■ia tuturor joburilor din Set■ri.

Chiria■i (admin)

Din **Utilizatori**, creezi un chiria■ (un cont web cu spa■iu propriu privat) cu un email ■i o cot■ de stocare. Fiecare rând î■i permite s■ deschizi, editezi sau ■tergi chiria■ul.

Editarea unui chiria■ · cote ■i suspendare FTP

În pagina de **Editare** a unui chiria■, schimbi emailul de recuperare sau cota, trimi■i un link de resetare a parolei sau setezi o parol■ nou■ ■i reactivezi FTP. Numele de utilizator nu poate fi schimbat.

Fiecare chiria■ poate avea o cot■ de stocare în GB (0 = nelimitat; chiria■ii noi au implicit 10 GB). La cot■ intr■ tot ce ■ine chiria■ul pe cutie: folderele lui FTP ■i seiful, împreun■. Când un chiria■ dep■■e■te cota, înc■rc■rile web sunt refuzate ■i autentific■rile FTP sunt suspendate automat, apoi restaurate automat când consumul scade sub limit■. Chiria■ul prime■te un email la ambele schimb■ri — mesajul de suspendare îi spune clar c■ backupurile trimise prin FTP nu se vor mai putea autentifica pân■ nu elibereaz■ spa■iu.

Rapoarte (admin)

Statistici de stocare ■i autentificare: capacitate ■i utilizare, ultima autentificare a fiec■rui utilizator cu IP ■i dispozitiv, ■i istoricul recent de autentific■ri. Expor■i în CSV sau PDF.

Resurse sistem (admin)

Pagina Rapoarte arat■ ■i starea în timp real a serverului: memoria (RAM) folosit■ vs. total■, num■rul de nuclee CPU cu procentajul de ocupare pe fiecare, ■i înc■rcarea medie (load average) — ca s■ vezi dintr-o privire cât de solicitat e serverul.

Jurnale (admin)

Un jurnal de diagnostic rotativ pentru streaming, acces media ■i erori. Îl vezi în aplica■ie sau îl gole■ti; se rote■te automat la 100 MB.

Set■ri

Î■i schimbi parola ■i emailul de contact. Adminii pot configura ■i contul de mail (SMTP) folosit pentru emailurile de resetare, App ID-ul receptorului Chromecast, Programatorul, dac■ FTP-ul cere criptare, domeniul ■i certificatul HTTPS, ora serverului (fus orar + NTP), firewallul de control al accesului ■i IPv6, ■i cât timp r■mân valabile linkurile temporare — fiecare descris mai jos.

Deconectare automat■ (admin): deconecteaz■ orice cont din panoul web dup■ o perioad■ de inactivitate (30 de minute implicit). Se aplic■ tuturor; cât e activ■, „■ine-m■ autentificat” este ascuns■ ■i ignorat■, deci o sesiune nu poate dep■■i timpul stabilit. E pornit■ implicit — oprirea ei e semnalat■ ca risc de securitate. O parol■ corect■ te autentific■ mereu, chiar imediat dup■ prea multe încerc■ri gre■ite, deci nimeni nu poate fi blocat din panou de cineva care îi ghice■te parola.

Or■ ■i dat■ — fus orar ■i NTP (admin)

Setezi fusul orar al serverului (alegi continentul, apoi ora■ul) ■i serverele de timp (NTP) de la care î■i sincronizeaz■ ceasul. Fiecare server de timp e verificat c■ r■spunde înainte de salvare, iar o linie de stare arat■ dac■ ceasul e sincronizat. Ora corect■ p■streaz■ exacte jurnalele, certificatele ■i rapoartele. Dac■ ceasul e mult deviat, folose■te **Sincronizeaz■ ceasul acum** — serviciul de timp din fundal corecteaz■ doar diferen■e mici ■i n-ar recupera singur o diferen■■ mare.

Re■ea — adres■ IP (admin)

Din **Set■ri** setezi IP-ul serverului: o adres■ fix■ (static■) sau automat■ (DHCP). Dup■ aplicare confirmi de la noua adres■ în 90 de secunde, altfel revine automat — deci o setare gre■it■ nu te blocheaz■.

Când accesezi exact IP-ul care se schimb■, e■ti dus automat la noua adres■; printr-un domeniu sau în spatele NAT se confirm■ singur dac■ adresa r■mâne accesibil■, ■i î■i aminte■te s■ îndrep■i întâi port-forward-ul din router c■tre noul IP (sau s■ confirmi din interiorul LAN).

Firewall ■i control acces (admin)

Restric■ionezi ce adrese surs■ pot ajunge la ma■in■: porne■ti filtrarea accesului ■i listezi IP-urile sau intervalele permise (CIDR). Adresa ta curent■ e mereu permis■, ca s■ nu te blochezi singur — iar dup■ ce aplici reguli noi, pagina confirm■ c■ e■ti în continuare conectat; dac■ nu poate, regulile anterioare sunt restaurate automat dup■ un minut.

IPv4 ■i IPv6 sunt afi■ate separat, citite din regulile pe care ma■ina le are efectiv înc■rcate. IPv6 e oprit dac■ nu î■ porne■ti din acela■i card — cât timp e oprit, aparatul nu are nicio adres■ IPv6. Lista accept■ atât intr■ri IPv4, cât ■i IPv6, iar fiecare se aplic■ pe familia ei. Cât timp se emite sau se reînnoie■te un certificat Let’s Encrypt, portul 80 e deschis pentru scurt timp pentru validare, iar modific■rile de firewall sunt refuzate în acel minut.

Actualiz■ri automate (admin)

Serverul verific■ zilnic dac■ exist■ o versiune nou■, semnat■ digital. Când exist■, o aplici cu un singur clic — o auto-actualizare sigur■ care înlocuie■te aplica■ia ■i reporne■te, p■strând toate datele, conturile ■i set■rile. Fiecare actualizare e verificat■ prin semn■tur■ ■i sum■ de control înainte de instalare, iar un watchdog de fundal revine automat la versiunea anterioar■ dac■ una nou■ nu porne■te.

Domeniu ■i certificat HTTPS (Let’s Encrypt)

Introduci domeniul ■i emailul ■i ceri un certificat Let’s Encrypt gratuit — securizeaz■ atât administrarea web (HTTPS), cât ■i FTP (FTPS) ■i se reînnoie■te automat. Îndreapt■ DNS-ul domeniului c■tre acest server înainte de a cere.

Instaleaz■ pe telefon (ca aplica■ie)

Android (Chrome): deschizi adresa HTTPS a aplica■iei, ape■i meniul ■, alegi „Instaleaz■ aplica■ia” / „Adaug■ la ecranul principal” ■i o porne■ti din noua pictogram■.

iPhone / iPad (Safari): deschizi adresa HTTPS în Safari, ape■i butonul Partajare, alegi „Adaug■ la ecranul principal”, apoi Adaug■. Ruleaz■ pe tot ecranul, ca o aplica■ie nativ■.

Conectare prin FTPS

Folose■te datele unui cont FTP cu un client care suport■ **FTP explicit peste TLS** (FTPS) în mod **pasiv**. Port de control **21**, porturi de date pasive **40000–40100** — deschide-le în firewall.

FileZilla / WinSCP: Gazd■, Port 21, Protocol FTP, Criptare „Require explicit FTP over TLS”, Tip logare Normal, apoi utilizatorul + parola contului; mod transfer Pasiv.

lftp: `lftp -u <user> ftps://<host>:21`

Securitate

FTP-ul e criptat implicit — FTPS e obligatoriu, iar autentific■rile FTP necriptate sunt refuzate. Un admin poate permite inten■ionat FTP necriptat din **Set■ri › Criptare FTP**, pentru un client care nu poate face FTPS; atunci parolele ■i fi■ierele circul■ în clar, deci e o ultim■ solu■ie.

Conturile FTP nu au shell ■i sunt blocate în propriul folder. Administrarea web e servit■ prin HTTPS, cu limitarea încerc■rilor de autentificare, protec■ie CSRF ■i izolare per chiria■.