Storage folder and self-test

All files lie in a storage folder. No download is handed out through the address of its file, but always through Fileshelf: Fileshelf first checks whether the visitor may get the file, then counts the download and sends the file. So that this cannot be bypassed, the folder must be locked against direct access.

The self-test

The dashboard checks the folder itself: Fileshelf places a test file and tries to fetch it through its address. It tests again after a day or when the folder changes; with “Allow software packages” on, every page of Fileshelf in the backend makes up for a missing test. The result comes in three colours:

Result	Meaning
Green	Protected: the files cannot be reached by their address, or the folder lies outside the web directory.
Red	Not protected: files can be downloaded past protection and counter. The dashboard shows how to close the folder.
Yellow	Not testable: the website did not answer the test request. Check again later.

Check now repeats the test, for example after you changed the server configuration.

Apache

Fileshelf places an `.htaccess` file into the folder. If the test stays red, your server does not allow `.htaccess` files. Ask your host to allow `AllowOverride` for this folder.

nginx

nginx does not read `.htaccess` files. Add the rule the dashboard shows to the server configuration (through your host if need be). For the default folder it reads:

```
location ^~ /fileshelf/ { deny all; }
```

Outside the web directory

Safest is a folder that has no address at all. Enter an absolute path outside the web directory under **Options → Storage → Storage folder**, for example `/home/customer/fileshelf`. Existing files are not moved when you change it – copy them into the new folder yourself.

> A menu item with the same alias as the storage folder (such as `fileshelf`) would be locked together with the folder. The dashboard warns in this case; give the menu item another alias.

Delivery by the web server

Under **Options → Storage → Delivery** you can let the web server send the file instead of PHP: *X-Sendfile* (Apache with mod_xsendfile) or *X-Accel-Redirect* (nginx with an internal address). Only choose this if your host has set it up; when in doubt, keep PHP. Protection and counter apply in all three cases.

Deutsche Fassung

Revision #3
Created 2026-11-09 22:53:56 UTC by Norbert Graup
Updated 2026-11-12 13:39:15 UTC by Norbert Graup