

Image Upload

Package manual · Secure frontend image upload for logged-in users (module) plus backend management of the uploaded images (component) – Joomla 5/6

1. Overview

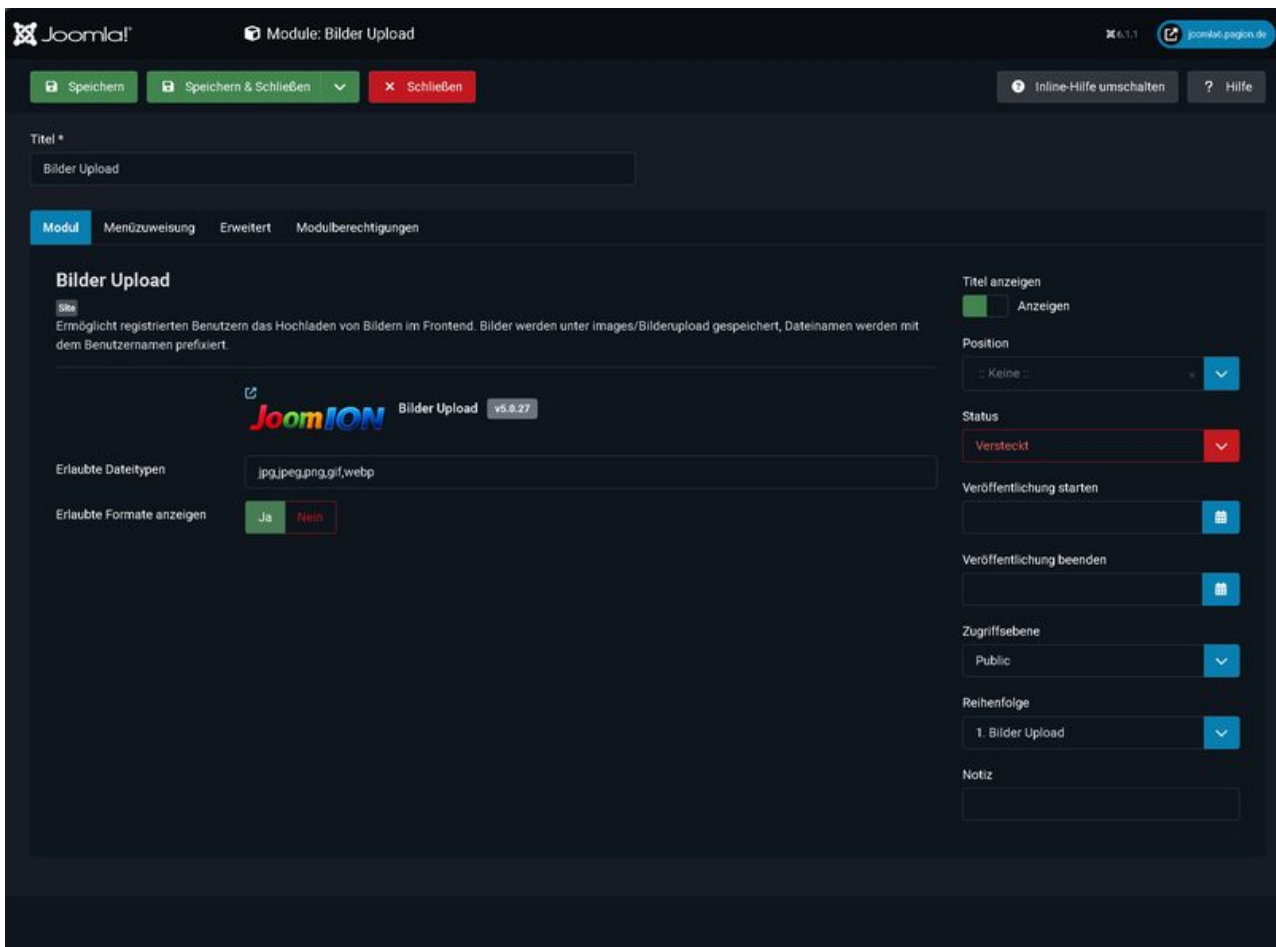
The **Image Upload** package installs two building blocks in one step:

- **Module** ``mod_bilderupload`` (frontend): an upload form through which **logged-in** users can upload images.
- **Component** ``com_bilderupload`` (backend): management of the uploaded images – view, download (individually or as a ZIP) and delete.

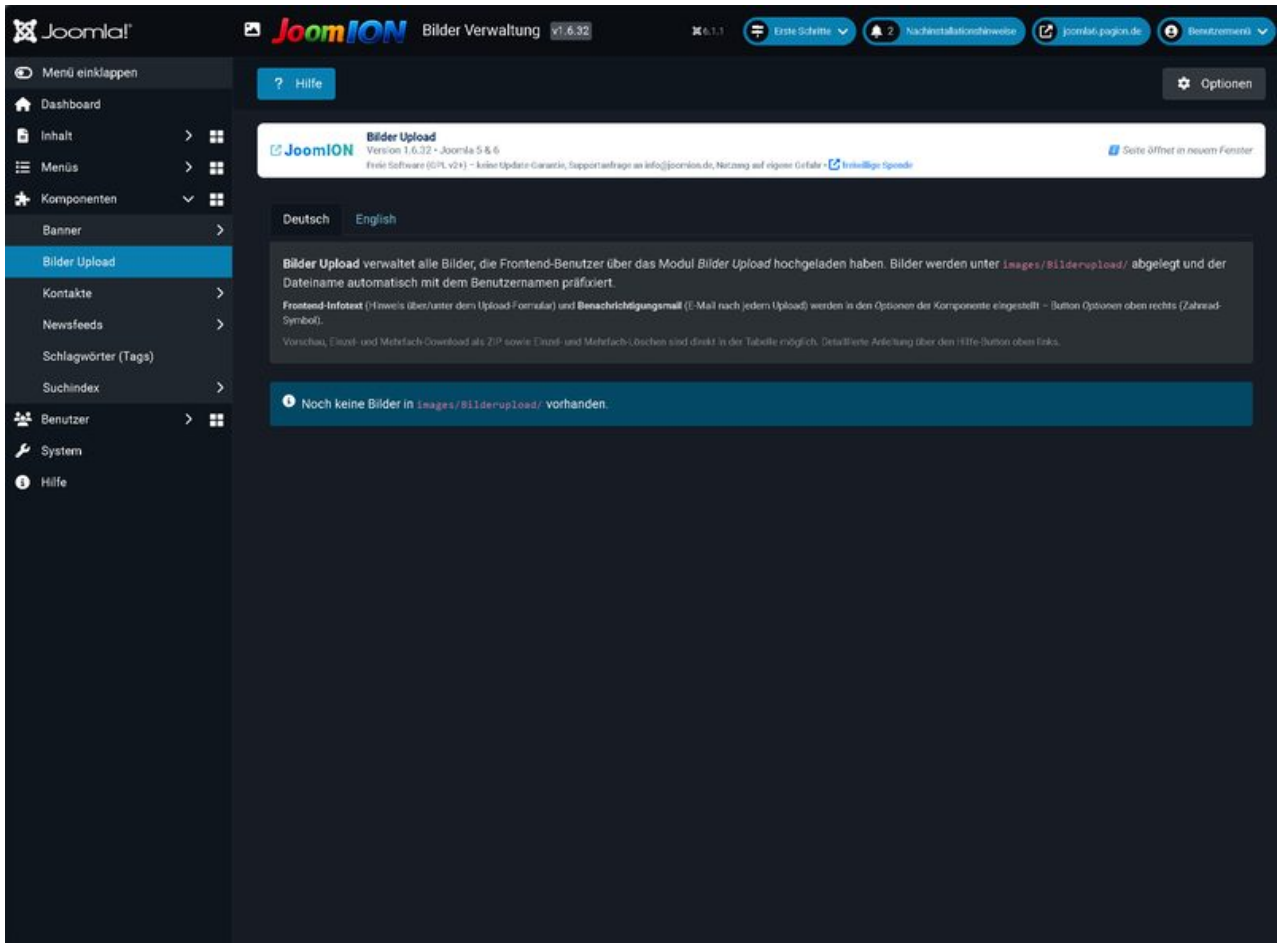
The files are stored in the directory `images/Bilderupload/` and named according to the scheme `username_filename.extension`.

2. Installation

- 1 Upload the package `pkg_bilderupload-X.zip` via **System** → **Install** (installs component + module).
- 2 Under **Content** → **Site Modules** create a new "Image Upload" module, assign a position and publish it (access: logged-in users/Registered).
- 3 Open the backend management under **Components** → **Image Upload**.



The "Image Upload" module in the frontend module editor

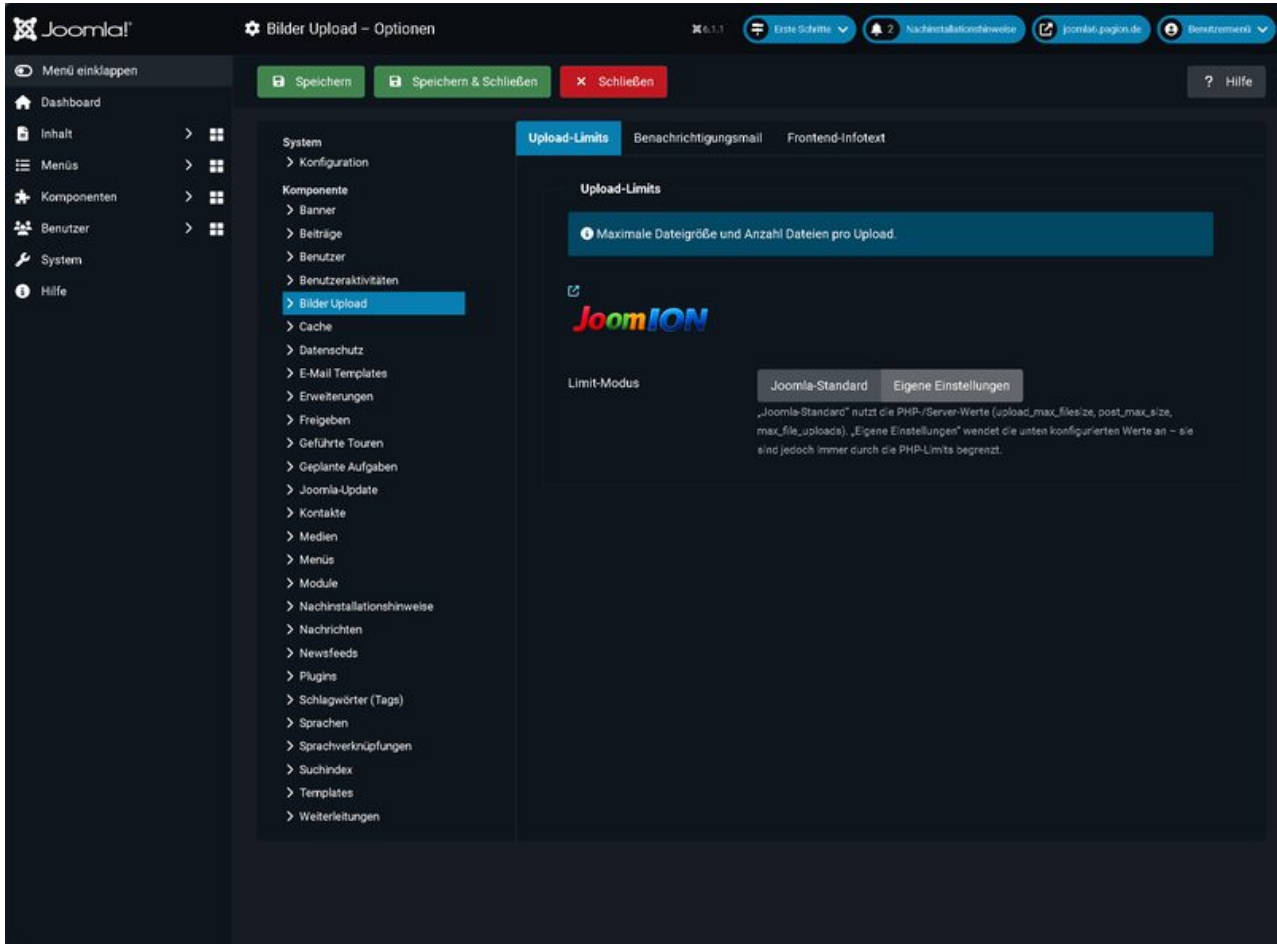


The "Image Upload" backend management view

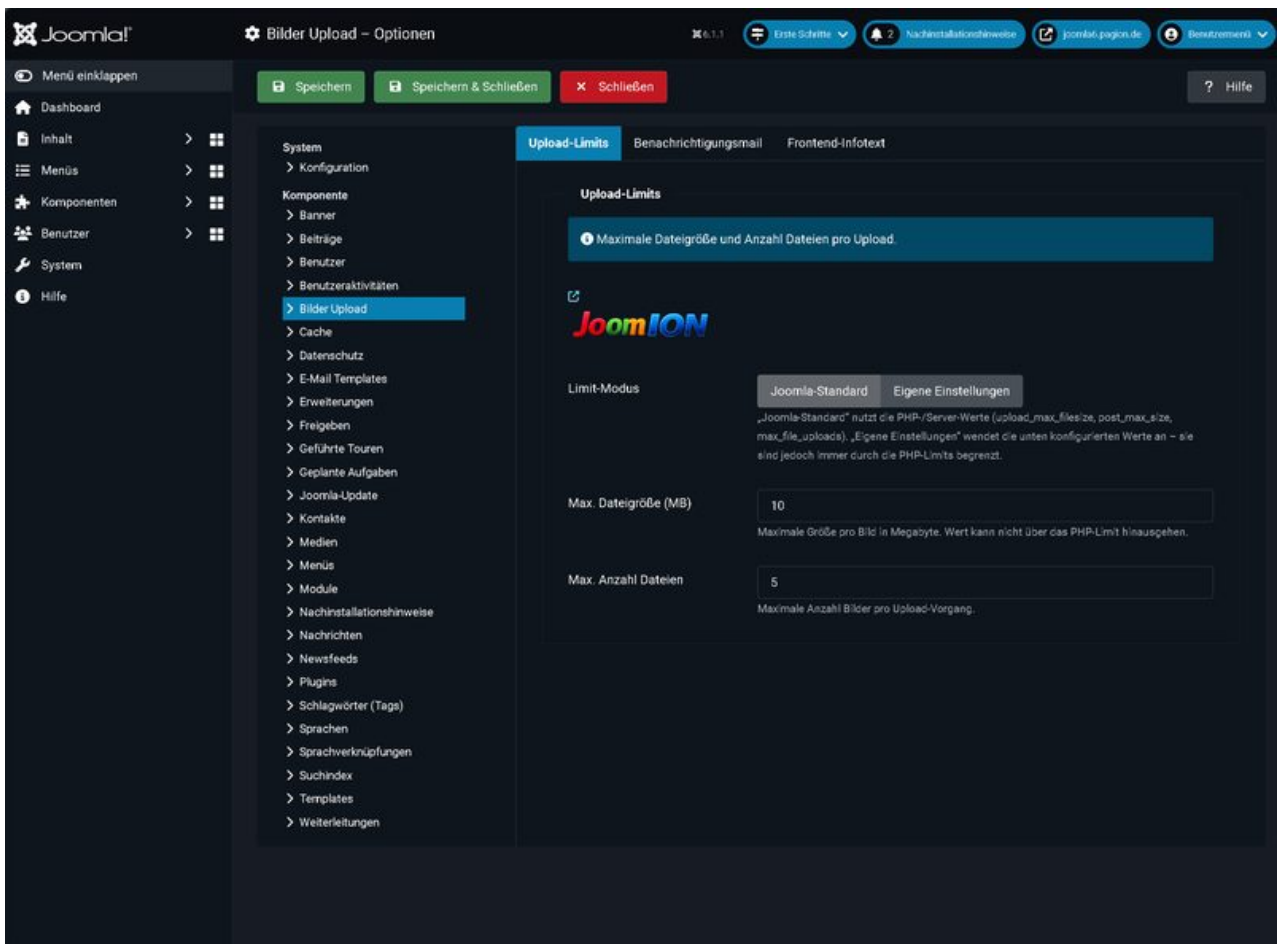
3. Settings (component options)

Via **Components** → **Image Upload** → **Options**:

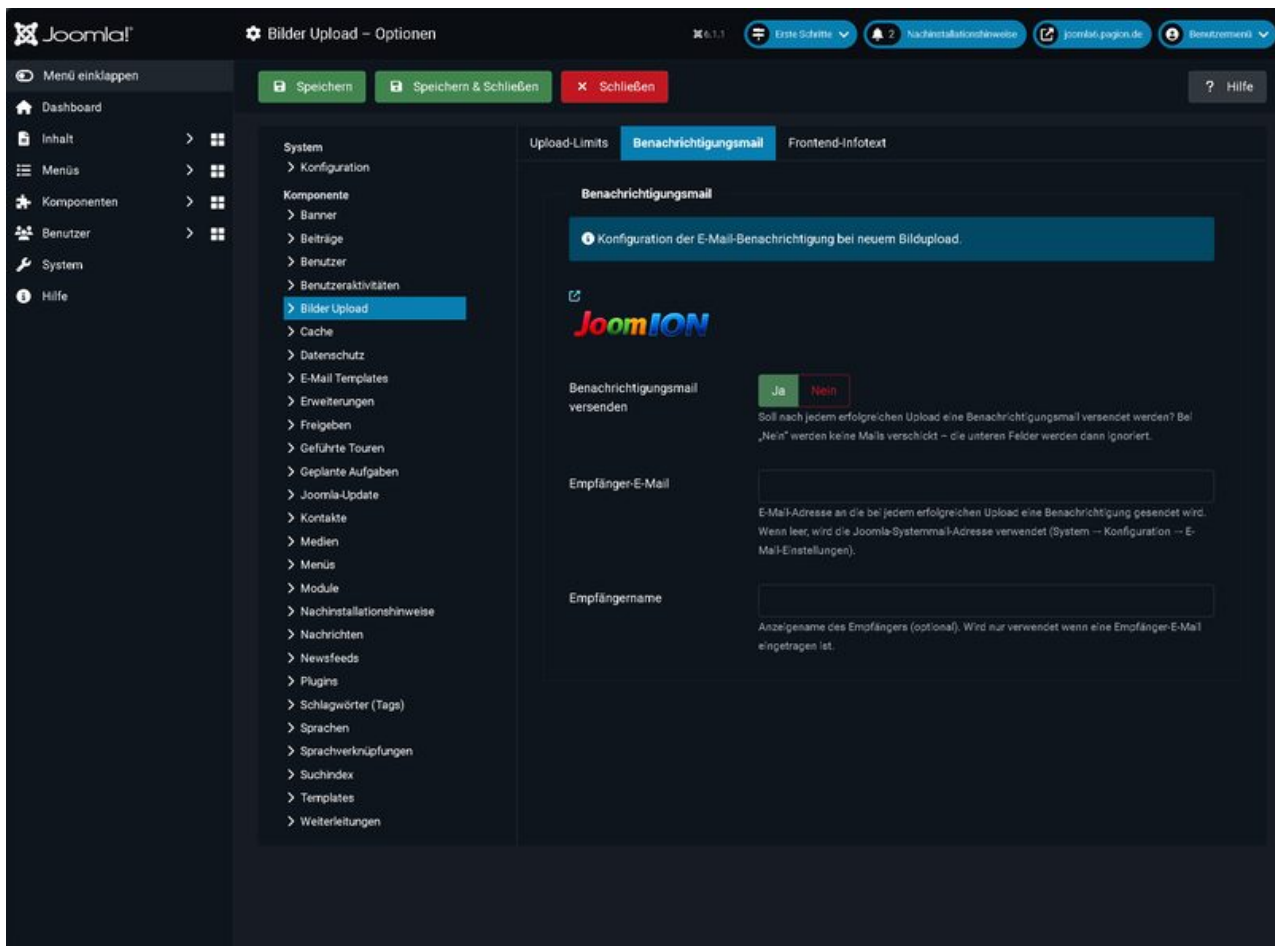
- **Upload limits:** maximum number of files per upload and maximum file size (MB).
- **Notification e-mail:** enable/disable plus recipient address and name (fallback: Joomla system mail).
- **Info text position:** above or below the upload form.



Upload limits in "Joomla standard" mode



Upload limits with "custom settings" (10 MB, 5 files)



Notification e-mail settings

The server-side limits `upload_max_filesize` and `post_max_size` (php.ini/.htaccess) apply additionally and cannot be raised in PHP at runtime. For large uploads, increase these values at your host.

4. Security

The upload is secured several ways (defense in depth):

- **CSRF token** and **mandatory login** – no guest upload.
- ``is_uploaded_file()`` + ``move_uploaded_file()`` (no include/move trick).
- **MIME check via magic bytes** (`finfo`), not via the browser-supplied value.
- **Whitelist** (image formats only) **and a hard blocklist** for executable/script/macro files – including double extensions like `image.php.jpg`.
- **File name sanitisation**, `basename()`, fixed permissions `0644`.
- ``.htaccess`` + ``.index.html`` in the upload folder (script execution disabled), set on install.
- **Delete/download** in the backend only via a `realpath()` check against the upload directory (no path traversal/symlink), with token and `core.manage` permission check.
- **E-mail** safe against header injection, all output XSS-escaped.

The package injects **no malicious code**: `_JEXEC` protection in all files, namespaced, Joomla 5/6 API. There are **no eval/shell** operations; database access uses bound parameters.

5. Licence, updates & donations

Free software (GPL v2+). The package is free of charge and needs **no licence key**. **No update guarantee**, **no guaranteed support** – use at your own risk. Support requests are welcome at info@joomion.de.

Updates are delivered normally through the **native Joomla updater** (System → Update → Extensions) – without any licence check.

If this package helps you, a **voluntary donation** on joomion.de is appreciated. Thank you!

6. Frontend usage

- 1 Log in as a registered user and open the page with the upload module.
- 2 Select one or more image files and upload them.
- 3 After a successful upload a confirmation appears; optionally a notification e-mail is sent to the operator.