Introduction to File Access (Pro)

File Access · https://publishpress.com/knowledge-base/regulate-file-url-access/

This feature requires the Pro version of the PublishPress Permissions plugin.

The "File Access" feature in the Pro version of PublishPress Permissions can control outside access to files in your WordPress Media Library. This means that you can block direct URL access to anything in your Media Library.

By default in WordPress, site visitors may blocked from accessing a post or page, but can still access any files in that post or page. If they know the URL for a private file, they will still be able to view and download it.

You can solve this with the "File Access" feature.

How to Protect Your Private Files

- Go to "Permissions" then "Settings", then "Features".
- Enable the "File Access" feature.

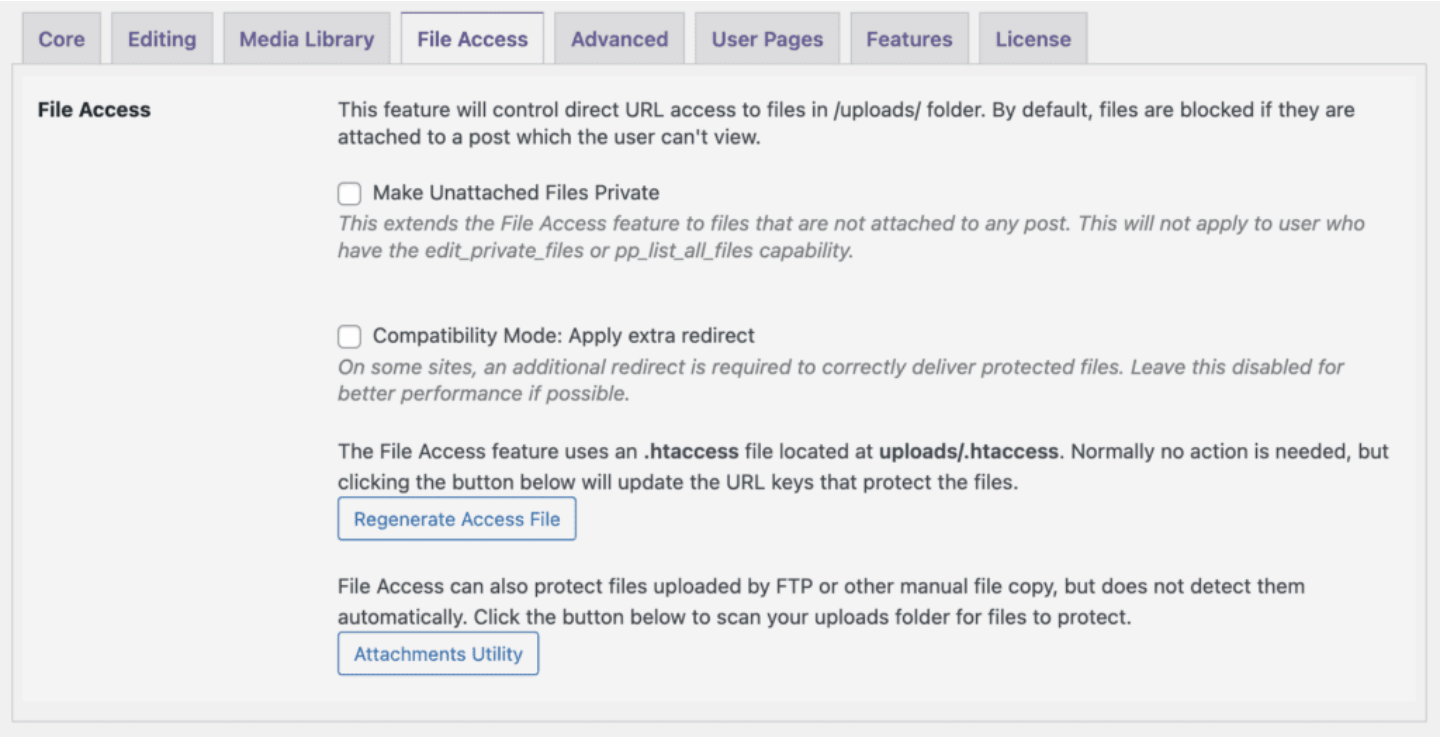
The File Access feature **will now start working immediately**. Now anyone who tries to visit the URL of a file they do not have access to will get a "404 - Page Not Found" error. Anything you do after this will be changing the settings around how the feature operates.

- Click the "File Access" tab.

There are several settings available on this screen:

- **Make Unattached Files Private**: This extends the File Access feature to files that are not attached to any post.
- **Compatibility Mode**: On some sites, an additional redirect is required to correctly protect files.
- **Regenerate Access File**: This option is there to reset the URL keys that protect the files. Clicking this button is rarely needed, but the PublishPress support staff may ask you to click this if the files

aren't being correctly protected.

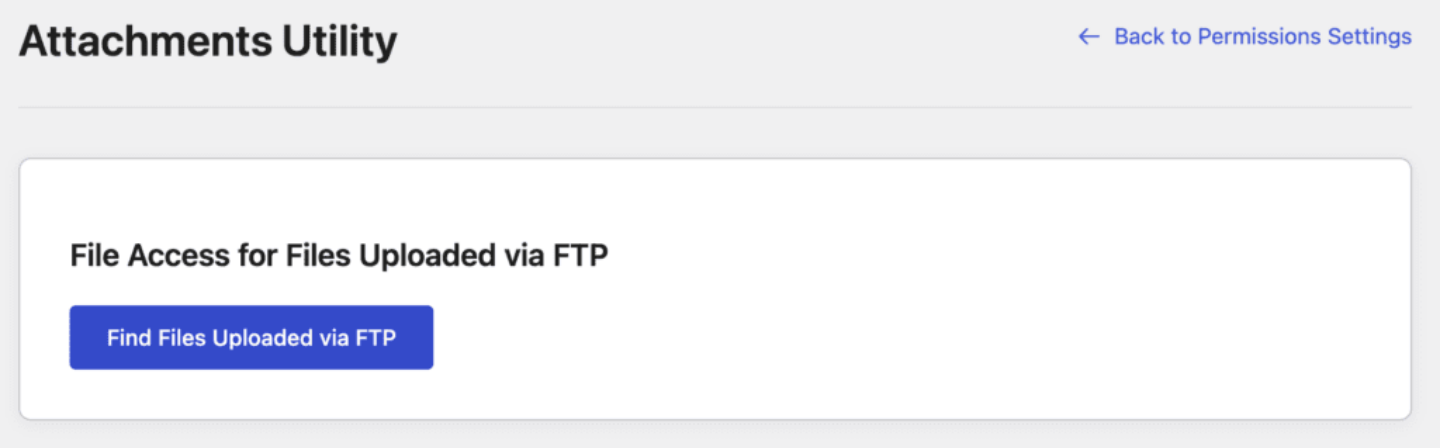


Filter Uploaded File

Attachments Utility

This File Access feature can protect files uploaded via FTP and WordPress methods that avoid using the WordPress Media Library. However, the files will not be filtered correctly until you run the "Attachment Utility".

- Click the "Attachments Utility" button.
- Click the "Find Files Uploaded via FTP" button.



Attachments Utility

How File Access Works

This File Access feature works by adding an .htaccess file to the `/wp-content/uploads/` folder.

So to be protected, a file must be inside `/wp-content/uploads/` or a subdirectory of it.

For each protected file, a separate RewriteRule is added to the `/wp-content/uploads/.htaccess` file.

File Protection Without .htaccess files

Nginx servers do not use an .htaccess file. To output Nginx rewrite rules, define the following constants in wp-config.php:

```
define( 'PP_NGINX_CFG_PATH', '/path/to/your/supplemental/file.conf' );
define( 'PP_FILE_ROOT', '/wp-content' );  // typical configuration (modify with actual path to folder your uploads folder is in, relative to http root)
```

You will need to provide your own server scripts to trigger an Nginx reload upon config file update.

On network installations, rules from all sites are inserted into the same file, specified by PP_NGINX_CFG_PATH. Each site's rules are preceded by a distinguishing comment tag.

To disable .htaccess output, define the following constant (in addition to PP_NGINX_CFG_PATH):

```
define( 'PP_NO_HTACCESS', true );
```

You may manually force regeneration of Nginx or .htaccess rules by creating the file defined in this constant:

```
define( 'PP_FILE_REGEN_TRIGGER', '/path/to/your/trigger/file' );
```