Admin Guide Articles

- Overview
- Adding or removing users from groups
- Adding a group
- Renaming a group
- Deleting a group
- Adding a user
- Independent admin users
- Deactivating a user
- Superuser
- Admin users
- Editing a user
- Deleting a user
- E-mail notification system
- File preview
- Time zone
- Overview
- File indexing and full-text searching
- ImageMagick thumbnail generation and image preview
- Accessing WebDAV
- Character encoding
- File Encryption
- Hiding file types for certain users or groups
- Custom authentication
- Joomla authentication
- Wordpress authentication
- Translating Web File Share
- The API
- Running custom scripts when users perform various actions
- Counting file downloads
- File reference
- Adding custom functionality
- Forcing certain file types to download
- Custom file actions
- Calculating MD5 Checksums
- Adding links to the menu
- Custom even scripts
- External Login Form
- Hiding options from the "Open with..." menu
- Automatic Login
- Custom "Open with" actions
- Custom CSS
- Resetting the FileRun superuser password
- Backup
- ZGL to ionCube
- Upgrading to PHP 5.4
- Migrating to another server
- Installing updates
- Upgrading PHP to version 7
- Changing the MySQL connection information
- Deleting old files
- Upgrading to PHP 5.5 or 5.6
- Overview

- Deleting a role
- Adding a role
- Editing a role
- Choosing A Hosting Service
- Installing ionCube on Top Hosting Providers
- Installing Ioncube Loaders
- Manual "ionCube" installation
- Activity notifications
- File-based Activity Logs
- Mozilla Thunderbird FileLink Addon
- Alternate downloads
- Metadata
- Desktop sync
- Mobile apps
- Upload problems
- Login problems
- Downloading problems
- Large files (>2GB)
- Metadata
- Configuring users’ file access

Overview

Groups can be used for:

1. Sharing a folder with multiple users at the same time. (You can also configure a user permissions so that it can only share folders with certain groups of users.)
2. Configuring e-mail notifications: adding notification rules involving multiple users at the same time.
3. Setting up admin users that can manage only certain groups of users.

Adding or removing users from groups

To add or remove a user from a group follow these steps:

1. Open the control panel.
2. Select “Users”.
3. Select the user you want to add to a group or remove from one.
4. Click “Edit user”
5. Using the “User group(s)” field, select only the groups that you want the user to be part of.
6. Click “Submit” to save the changes.

Adding a group

To create a new group follow these steps:

1. Open the control Panle
2. Select "Groups".
3. Click 'Create New".
4. Fill in the form
5. Required Field -'Group Name'
6. Click “Submit” to create the group with the specified details.

Renaming a group

To change a group's name follow these steps:

1. Open the control panel.
2. Select “Groups”.
3. Select the group that you want to rename
4. Click “Edit group”
5. Make the appropriate changes in the form.
6. Click “Save” to save the changes.

Deleting a group

To delete a group follow these steps:

1. Open the control panel.
2. Select “Groups”.
3. Select the group you want to remove.
4. Click “Delete group”.
5. Click “Delete” to confirm the group's deletion.

- Deleting a group **does not** delete the users contained.

Adding a user

To create a new user account follow these steps:

1. Open the control panel.
2. Select “Users”.
3. Click “Create new”.
4. Fill in the form:
5. Required fields:
   - Username
   - Name
   - Home folder
6. Click “Submit” to create the user with the specified options.

Click the “Check path” link next to the “Home folder” field, to make sure the path you've set for him points to an existing folder. If it doesn't, the user will see an error message after logging in.

Setting Home folder path

Please use only forward slashes (/) when setting up paths, even if you are running a Microsoft Windows server. If you are not sure how the path should look like, look at your own home folder path which is displayed on the form, inside the read-only field "*Your personal home folder is*".

Independent admin users

Independent admin users can:

1. See and manage only user accounts, roles and groups created by themselves.
2. See and manage only his e-mail notification settings.
3. Browse his own users' activity logs.
4. Manage his own metadata settings.

When configuring the independent admin's permissions, you can choose:

1. How many user accounts he will be able to create.
2. Whether he will be able to define the path of the users' home folder, or if he will be limited to a specified folder. If you define a “Home folder template path” for the independent admin user, he will not have any home folder related options when adding a new user. If you leave the field blank, all the users he creates will have their home folders automatically created inside the admin's own home folder.

Also, an independent admin user is required to configure space and traffic quotas for the users he creates. He cannot assign more space and traffic then it was assigned for its own account.

Deactivating a user

To deactivate a user account follow these steps:

1. Open the control panel.
2. Select “Users”.
3. Select the user you want to deactivate.
4. Click “Deactivate user account”.

Following these steps again it will reactivate the user account. This can be be used to temporary disable one user's access to FileRun.

Superuser

The superuser is the first account that is automatically created at FileRun installation. Its default username is “admin”.

Along the administrative tasks the other admin users can do, he is the only user that can:

1. Change the system's configuration.
2. Install software updates.
3. Install license upgrades.

The superuser account cannot be deleted or deactivated. It can however be renamed.

It is highly recommended that you do not assign a role to the superuser account.

Admin users

Admin users can:

1. Manage user accounts, except their own and other admins' accounts.
2. Manage roles.
3. Manage user groups.
4. Manage e-mail notification settings.
5. Browse users' activity logs.
6. Manage metadata settings.

When configuring the admin's permissions, you can choose:

1. What administrative section is he allowed to access.
2. Which groups of users he can see and manage.
3. Whether he will be able to define the path of the users' home folder, or if he will be limited to a specified folder.

Editing a user

To edit a user account follow these steps:

1. Open the control panel.
2. Select “Users”.
3. Select the user you want to edit.
4. Click “Edit user”
5. Make the appropriate changes in the form.
6. Click “Submit” to save the changes.

Deleting a user

To delete a user account follow these steps:

1. Open the control panel.
2. Select “Users”.
3. Select the user you want to remove.
4. Click “Delete user”.
5. Click “Delete” to confirm the user's deletion.

Deleting a FileRun user account does not remove the user's home folder or its activity log entries.

What gets deleted:

- his “Deleted files” folder
- the WebLinks he created
- the folder sharing information

E-mail notification system

Configuration

To be able to send e-mails from Web File Share, you need to either have PHP configured with “sendmail” or have Web File Share configured with an SMTP server. Do note that most SMTP servers require authentication, and to prevent spam and other attacks, some don't even allow you to send e-mails from other addresses than the one configured for authentication. So don't be surprised if you are trying to send a file from a particular e-mail address and the recipient sees the message as coming from the address you used for the SMTP authentication.

Web File Share tries to detect your SMTP server configuration and in some cases will use STARTTLS even if you don't want to. If that is the case, the solution is to open the file customizables/config.php (create the file if it doesn't exist) in a text editor and edit it too look like this:

<?php $config['system']['email']
['smtp_options'] = ['SMTPAutoTLS' => false, 'ssl' => ['verify_peer' => false, 'verify_peer_name' =>false,'allow_self_sig

Introduction

There are three ways you can configure Web File Share to send e-mail notifications:

(1) Admin users can enable or disable the “Notifications” checkbox for the users, when they create or edit their accounts. In this case the users will receive e-mail notification messages when files are upload or downloaded from their folders or when comments are attached to their files, or when other users share folders with them. The users also have control over this option and they can enable/disable from their “Account settings” panel. One requirement from e-mail notifications to be sent on other users action is the permission to “see and exchange files with”. This is set from the control panel, under the “Permissions” tab, when editing a user account. If user A isn't aware of the existence of user B, user A will not be notified if user B makes changes inside user A's folders.

(2) Admin users can also use the “Control Panel » Notifications” section for setting up rules for notifications. Here you manually select which user-performed actions should send e-mail notifications. Using this option you can configure e-mail notifications to be sent to different e-mail addresses than the ones set for the user accounts.

(3) With the Enterprise Web File Share version, users can choose to be notified when certain actions are being performed in a particular folder, by right-clicking the folder and selecting the “Notifications” option. The users can choose to be notified only about “write” actions or “read” actions. This option allows the users to receive notifications about “write” actions performed in folders that do not belong to them, but have been shared by other users, so the users can get notified when new files are available in these folders.

By default the e-mail notifications messages are sent from the e-mail address “some@email-address.com”. We recommend you to change that (from “Control Panel » System configuration » E-mail settings”) as many e-mail servers do not process messages that come from addresses that use a different domain name then the one used to host the Web File Share installation. In most cases this e-mail address needs to be associated with a valid e-mail account.

Customizing the notification messages

There are more than 70 actions that Web File Share can monitor in order to send e-mail notifications. Each action can have its own e-mail body template. For each action there is a corresponding template file, located inside the folder “customizables/emails/“. For the actions that do not have a template file, the template “customizables/emails/generic.tpl.txt” will be automatically used.

The following information which applies to all outgoing notifications can be customized from the control panel, under “System configuration”, “E-mail”, “Settings”:

- From e-mail address
- An optional BCC (Blind carbon copy) e-mail address
- E-mail subject
- Body content

E-mail template file format

```
<Action>
 [...]
 User "{$info.userInfo.name}" has performed the following action: "{$info.details.action}
 [...]
</Action>
```

The XML tags (<Action>, <From>, <Subject>, etc...) should not be altered or removed from the template files.

The body of the notifications contains Smarty syntax that allows you to use variables and perform various logical operations. For more details on using Smarty, please check this page: http://www.smarty.net/docs/en/smarty.for.designers.tpl

The following Smarty variables are available for use inside the templates:

{$info.userInfo.username}	User's login name.
{$info.userInfo.name}	User's name.
{$info.userInfo.company}	Company name
{$info.userInfo.website}	User's website address.
{$info.userInfo.description}	User's admin note.
{$info.config.url.root}	The URL of the Quik File Share installation.
{$info.settings}	Array containing Quik File Share's current settings.
{$info.details}	Array containing details related to the performed action. The structure varies according to each specific action.

Adding an email notification template

Each action has a unique keyname. Here are two examples:

- "upload" for "When a file gets uploaded."
- "download" for "When a file gets downloaded").

(You can check the following table for a full list of keynames.)

To add a custom template for a certain action, a text file named "keyname.tpl.txt" should be created in the e-mail notifications templates folder (as pointed above).

Actions keynames

Used often	
upload	File uploaded
receive_upload	File received (via upload)
receive_copy	File received (via copy)
receive_move	File received (via move)
download	File downloaded
provide_download	File downloaded by other user
weblink_access	WebLink folder access
weblink_download	WebLink download
weblink_upload	File received (via WebLink)
shared_folder_available	New shared folder available
comment_added	File comment added
comment_received	Comment received on a file from other user

metadata_changed	Metadata information changed for a file
login	Login
folder_shared	Folder shared
weblink_create	WebLink created
file_encrypted	File encrypted
file_decrypted	File decrypted
Rarely used	
weblink_update	WebLink modified
weblink_remove	WebLink removed
logout	Logout
login_failed	Login failed
login_failed_account_deactivated	Account deactivated
password_changed	Password changed
user_manually_activated	Account activated by admin user
user_manually_deactivated	Account deactivated by admin user
comment_removed	File comment removed
folder_unshared	Folder unshared
Successful file actions	
file_moved	File moved
file_copied	File copied
file_deleted	File deleted
deleted_file_restored	Restored deleted file
trash_delete_file	File permanently deleted
file_renamed	File renamed
zip_files	Files zipped
files_send_by_email	Files sent by email
file_locked	File locked
file_unlocked	File unlocked
version_restored	File version restored
version_deleted	File version deleted
Successful folder actions	
new_folder	New folder created
folder_moved	Folder moved
folder_deleted	Folder deleted
deleted_folder_restored	Restored deleted folder
trash_delete_folder	Folder permanently deleted
folder_renamed	Folder renamed
folder_copied	Folder copied
zip_folder	Folder zipped
Failed file actions	
upload_failed	Upload failed
file_copy_failed	Failed to copy file
file_deletion_failed	Failed to delete file
file_move_failed	Failed to move file
failed_file_rename	Failed to rename file
zip_files_failed	Failed to zip files
files_send_by_email_failed	Failed to send files by email
file_lock_failed	Failed to lock file
file_unlock_failed	Failed to unlock file
failed_to_add_comment	Failed to add comment to file

failed_to_remove_comment	Failed to remove comment from file
version_restoration_failed	Failed to restore file version
version_deletion_failed	Failed to delete file version
Failed folder actions	
new_folder_failed	Failed to create new folder
failed_folder_rename	Failed to rename folder
folder_copy_failed	Failed to copy folder
folder_deletion_failed	Failed to delete folder
folder_move_failed	Failed to move folder
zip_folder_failed	Failed to zip folder
Misc	
new_user_registration	New user registration
password_changed	Password changed
password_recovery	Password recovery
Administrative	
user_added	User added
user_edited	User edited
user_deleted	User deleted
role_added	Role added
role_edited	Role edited
role_deleted	Role deleted
space_quota_warning	Space quota usage warning

Grouping notifications

You can configure Web File Share to send all the notifications for a certain time period in a single e-mail message. This helps preventing Web File Share from sending hundreds of e-mail messages at a time, when users are uploading many files in a short time span.

To enable this you need to uncheck the option ”Instant email notifications“ available in “Control Panel” » “System configuration” » “E-mail settings”. The notifications will no longer be sent instantly, but queued until you run the script “cron/email_notifications.php” from the command line. On most Linux servers the command looks like this:

```
php cron/email_notifications.php your.server.hostname.com
```

In some cases, where you have a custom “php.ini” PHP configuration file for the Web File Share installation folder you might need to specify the path to it, so that the command is executed with the same configuration and not the default one (which usually doesn't load needed extensions, such as ionCube):

```
php -c php.ini cron/email_notifications.php your.server.hostname.com
```

Using a Cron job on Linux servers or a scheduled task on Windows, you can choose the time interval the e-mail notifications are getting sent.

You can read more about cron here: http://en.wikipedia.org/wiki/Cron For examples, see this page: http://www.thegeekstuff.com/2009/06/15-practical-crontab-examples/

If you are using a web hosting service, you most probably have a control panel tool for setting up scheduled tasks, so we recommend you to ask your server administrator or hosting service tech support how do you go about setting this up.

File preview

Previewing documents

The following file types can be previewed or opened with Web File Share by default:

Image files:

- PHP GD extension: jpg, jpeg, gif, png, jpe
- ImageMagick: most known image file types

Office documents:

- PDF documents are opened inside the browser, on most browsers, and in some which don't support that, open with Web File Share's HTML5-based PDF viewer.
- rtf, doc, xls, pps, ppt, docx, xlsx, pptx, odp, fodp, ods, fods, odt, fodt, sxw, sxc, sxi open by default with Box View
- odp, ods, odt open with Web File Share's own OpenDocument Viewer
- EPS documents can be previewed with ImageMagick: ImageMagick_thumbnail_generation_and_image_preview

Text documents:

- svg, class, h, bat, cmd, sh, eml, txt, readme, nfo, htaccess, htm, html, cfm, wml, htt, inc, vbs, js, json, java, jsp, jspx, asp, aspx, ashx, asmx, axd, pl, cgi, php, php3, php4, py, rb, rhtml, erb, pxp, xml, xhtml, sass, css, tpl, sql, sub, srt, log, ini (new extensions can be easly added)

Archive files:

- ZIP, TAR, TAR.BZ2, TBZ, BZ2, TAR.GZ, TGZ, JAR archives and GZ compressed files can be extracted.

Video files:

- mpg, mov, webm, mp4, swf, flv, ogv, m4v
- wmv (usually supported only by Windows computers) - not an official Web File Share feature because of third-party software requirements

Audio files:

- mp3, mpa, m3u, m3u8, pls, ogg, wav, flac

AutoCAD files:

- skp, fbx, dwg, dwf, dxf, rvt

Misc file types:

- URL (opens the web page inside an embedded window)

Third party Online services

Additional preview methods will be displayed in the contextual menu, under “Open with..”, when certain actions can be performed for the selected file.

Google Docs Viewer and Editor

- can preview, create and edit most common office file types

Microsoft Office Web Viewer (http://officewebviewer.com)

- can preview most common Microsoft Office file types

Zoho Editor (http://www.zoho.com/)

- can preview, create and edit most common office file types

Aviary Image Editor (http://www.aviary.com/)

- Available for: “jpg”, “jpeg”, “png”

Pixlr Image Editor (http://www.pixlr.com/)

- Available for: “jpg”, “jpeg”, “gif”, “png”, “psd

Autodesk Freewheel Viewer (http://labs.autodesk.com/technologies/freewheel/)

- available for AutoCAD documents

Google Earth KML Viewer

- available for “kml” files

Bing Maps KML Viewer

- available for “kml” files

Cloud Convert

- available for converting many common file types

Hiding Preview Options

Most preview plugins can be disabled from the control panel, under “System configuration” » “Files” » “Open with.. options”

Setting Default Open Method

You can choose how Web File Share handles each type of file. Simply access the control panel, under “System configuration” » “Files” » “Open with.. options” » “Defaults”

Time zone

When using Web File Share with a webhosting service, sometimes the server is located in a different time zone than you and your users. You can adjust the time difference by configuring Web File Share to use your time zone instead:

Open the file "*/path-to-WebFileShare/*customizables/config.php" in a text editor and add the following line:

```
date_default_timezone_set("Asia/Tokyo");
```

Replace "Asia/Tokyo" with your desired location.

Find a list of available timezone codes for various locations on the planet at
http://www.php.net/manual/en/timezones.php

Date/Time Formats

If you also want to change the date/time formats used in the interface, these can be changed by editing the language translation files (See Translating Web File Share).

Overview

Most of the configuration is done from Web File Share's control panel. However, there are additional configuration options that can be set by editing the file “customizables/config.php”. If the files does not exist, you can simply create it.

User Interface

$config['app']['ui']['custom_css_url'] = 'custom.css';	Loads an additional CSS file with your customizations. It's better to do this than edit Web File Share's existing CSS code.
$config['app']['ui']['enable_favicon_ico'] = true;	Allows browsers to use the file “favicon.ico” for the bookmark icon.
$config['app']['ui']['ReadMeFileName'] = "README";	Sets the name of the file that is used for displaying folder information.
$config['app']['hidden_file_names'][] = "*.exe";	Hides all files who's names are ending with “.exe”. You can add multiple configuration lines like this one, to hide additional files.
$config['app']['hidden_folder_names'][] = "_*";	Hides all folders who's names are starting with “_”. You can add multiple configuration lines like this one, to hide additional folders.
$config['app']['upload']['max_simultaneous'] = 5;	Change the number of files Web File Share is simultaneously uploading. The default number is 3. As a rule of thumb, the larger your files, the smaller this number, and vice-versa.
$config['app']['labels']['default'] = [['color' => 'green', 'text' => 'APPROVED'], ['color' => 'orange', 'text' => 'PENDING'], ['color' => 'red', 'text' => 'REJECTED']];	These are the default labels, which can be customized as desired.
$config['imagemagick']['older_than_6_3_2'] = true;	Use when the version of ImageMagick ont he server is older than 6.3.2, or if the file previews are not centered inside the thumbnails, but aligned on the left side.
$config['app']['thumbs']['output_small_filesize'] = 8388608;	By default, images smaller than 8MB are send directly to the browser instead of having a thumbnail generated. You can alter this limit.
$config['imagemagick']['fileSizeLimit'] = 1048576;	Limits the ImageMagick thumbnail generation only for files larger than 1048576 bytes (1MB).
$config['app']['disable_sound_notification'] = true;	Sets the default state of the sound notifications to off.
$config['app']['media']['music']['latest']['limit'] = 100; $config['app']['media']['music']['random']['limit'] = 100; $config['app']['media']['photos']['latest']['limit'] = 100; $config['app']['media']['photos']['tags']['limit'] = 100;	Customize various media folder listing limits.
$config['app']['metadata']['search']['results']['limit'] = 200;	Customize the number of files listed in the search-by-metadata result
$config['app']['metadata']['search']['results']['limit'] = 200;	Customize the number of files listed in the search-by-metadata result
$config['app']['ui']['login_logos']['acme'] = 'https://www.acne.com/logo.png';	Access the Web File Share installation URL by appending “?client=acme” to show that particular pre-configured logo instead of the default configured one.

File indexing and full-text searching

Web File Share configuration

You can enable the full-text file searching from “Control Panel” » “System configuration” » “Files” » “Indexing”. It is not enabled by default because it requires third-party software (Apache Tika).

If you are running Tika in command line mode, simply provide the path to the “tika-app-1.12.jar” file. That's it! Click the “Check path” to make sure it works. If Java is installed on the server and the file path is correct, you should see the Apache Tika version displayed as a result of the test.

If you are running Tika in server mode, provide the hostname and port number of the Tika server. Click the “Test server” to make sure it works. If everything is in order you should see the Apache Tika version displayed as a result of the test.

Installing Apache Tika

Installing Tika is as simple as uploading a file to your server.

Download the “jar” file from here: https://tika.apache.org/download.html

Download the “tika-app[*].jar” if you want to run Tika from the command line and “tika-server[*].jar” if you want to run it as a server. Running Tika in server mode speeds up the indexing process.

You can read more about Tika here: https://tika.apache.org

Set Index Queue Manager

As extracting the text from a binary file requires a lot of CPU processing, the files are queued and processed one at a time. This requires the script “cron/process_search_index_queue.php” to be executed frequently. We recommend running the script every 5 minutes or so, so you will not have to wait to long until an uploaded file will be found by the search engine.

On a Linux server this can easily be done be setting up a cron job like this:

1. Create a new text file at “cron/process_search_index_queue.sh” and write the following inside:

   ```
   php -c php.ini process_search_index_queue.php
   ```

   To find out the path of the “php.ini” used by Web File Share open “http://your-site.com/WebFileShare/info.php” file in your browser.
2. Open a command line console (SSH)
3. Open the crontab editor by running:

   ```
   crontab -e
   ```

4. Write:

   ```
   * * * * * /path-to-WebFileShare/cron/process_search_index_queue.sh
   ```

5. Press “:wq” and “Enter” to save the changes and close the editor.

If your hosting service is running the cPanel administrative tool, it usually provides a web-based tool for setting up cron jobs easier.

On Windows this can be achieved by creating a Windows schedule event which calls a .BAT file containing something like this:

```
CD cron
C:/PHP/PHP.EXE process_search_index_queue.php
```

ImageMagick thumbnail generation and image preview

Introduction

Web File Share can make use of ImageMagick utility for generating image thumbnails and previews for PDF, PSD and other advanced file formats. ImageMagick also enables support for large (high-res) pictures in Web File Share.

GraphicsMagick (http://www.graphicsmagick.org) can also be used, and in some cases it can be faster and more efficient than ImageMagick

Installing ImageMagick

Please see http://www.imagemagick.org

Hewlett-Packard Graphics Language (HPGL) plotter files (.plt) can also be previewed with Web File Share and ImageMagick by installing “Hp2xx” (http://www.gnu.org/software/hp2xx/hp2xx.html). Windows version available here: http://gnuwin32.sourceforge.net/packages/hp2xx.htm

If you are running a Windows server, we recommend you to install ImageMagick to a path without space characters (like “Program Files”). You can install it for example to a path like “C:/ImageMagick”.

PDF Support

For ImageMagick to be able to generate thumbnails for PDF documents you will also need to install Ghostscript (http://www.ghostscript.com/download/gsdnld.html).

Setting up Web File Share

To enable ImageMagick please follow these steps:

1. Login as superuser (default username “admin”).
2. Open “Control Panel”.
3. Go to “System configuration” » “File preview and thumbnails”.
4. Enable ImageMagick.
5. Set path to ImageMagick “convert” binary.

Example of valid paths:

```
Windows servers: C:/ImageMagick/convert.exe
Windows servers: C:/"Program Files"/ImageMagick/convert.exe
Linux servers: /usr/bin/convert
```

Troubleshooting

If you see broken icons instead of thumbnails:

1. Make sure ImageMagick is working, running the following command: convert logo: image.jpg
2. Make sure that Ghostscript is working. Try converting a PDF document using the command line: convert example.pdf example.png
3. Make sure the path to ImageMagick is correctly configured in Web File Share's control panel.
4. On Windows servers, make sure PHP can run external application. You need to give the Internet Guest User (IUSR_<your-computer-name>) “read & execute” permission on the file that PHP is trying to run ImageMagick trough. That would be “cmd.exe” (located usually inside the folder “C:/Windows/System32”), the file used for running programs trough the command line.

Accessing WebDAV

As an alternative, Web File Share can be also accessed with a standards-compliant WebDAV application. This can be useful for managing the remote files as they are folders on the local computer.

WebDAV client programs tested with Web File Share:

Program Name	Operating System	License	Notes
MacOS Finder	MacOS		Guide available down on this page.
Cyberduck	MacOS	Free	
WebDrive	Windows/MacOS	Free Trial	Recommended by Web File Share!
NetDrive	Windows	Free For Personal Use	
IT Hit "Map Drive"	Windows	Commercial	
GoodSync	Windows/MacOS/Android/iOS	Free/Pro versions	Good for two-ways folder synchronization
WebDAV Navigator	iOS	Free	
WebDAV-Sync	Any (Java)	Open-source	Command-line tool for two-ways folder synchronization. Works great.
DAVbox	Any (Java)	Commercial	Works great for two-ways folder synchronization.

An example of the URL you need to use to access Web File Share's WebDAV would be: http://demo.webfileshare.com/dav.php/ (for our online demo)

Please note that the URL must contain the trailing slash character, after “dav.php”.

MacOS: Connecting with Finder

Assuming your Web File Share instance is installed at https://www.your-site.com/webfileshare

In the Finder, choose Go > Connect to Server, type the address of the server in the Server Address field, and click Connect. The server address should be in a form similar to this: ADDRESS/webfileshare/dav.php/.

For our example, that would be:

https://www.your-site.com/webfileshare/dav.php/

For details, check the respective vendor documentation at the Apple website:http://support.apple.com/kb/PH3857

Linux: mounting from the command line

Install the WebDAV support using the davfs package. On Debian/Ubuntu, you can use:

```
sudo apt-get install davfs2
```

Reconfigure davfs2 to allow access to normal users (select Yes when prompted):

```
sudo dpkg-reconfigure davfs2
```

Add the users you want to be able to mount the share to the davfs2 group:

```
sudo usermod -aG davfs2 <user>
```

Edit /etc/fstab and add the following line for each user who wants to mount the folder (with your details where appropriate):

```
your-site.com/webfileshare/dav.php/ /home/<username>/webfileshare davfs user,rw,noauto 0 0
```

Then, as each user who wants to mount the folder:

Create the folders webfileshare/ and .davfs2/ in your home directory

Create the file secrets inside .davfs2/, fill it with the following (with your credentials where appropriate):

```
your-site.com/webfileshare/dav.php/ <username> <password>
```

Ensure the file is only writable by you either through the file manager, or via:

```
chmod 600 ~/.davfs2/secrets
```

Run the command:

```
mount ~/webfileshare
```

To automatically mount the folder on login, add the command you used in step 4 to ./.coderc

Known Issues

Problem: Resource temporarily unavailable

Solution: If you experience trouble when you create a file in the directory, edit /etc/davfs2/davfs2.conf and add:

```
use_locks 0
```

Problem: Certificate warnings

Solution: If you use a self-signed certificate, you will get a warning. If you are willing to take the risk of a man in the middle attack, run this command instead:

```
echo "y" | mount ~/webfileshare > /dev/null 2>&1
```

Character encoding

As PHP 5 does not have support for Unicode filenames, Web File Share can handle filenames that use one particular encoding. By default, Web File Share is configured to convert the text to UTF-8. This allows the users to upload files with names in any language, containing any non-English character. The filenames will look properly in the browser and the user will be able o manage them. The down-side is that, on some operating systems such as MS Windows, when using FTP or other methods of accessing the files directly in the filesystem, the names might not look as expected. For example, if the user uploads with Web File Share a file named "Iñtërnâtiônàlizætiøn.zip", when accessing the folder by FTP, the file's name will look something like this "lÃ±tÃ«rnÃ¢tiÃ´nÃlizÃ¦tiÃ¸n.zip".

Zip archives

As Web File Share will not alter in any ways the contents of the uploaded files, the filenames inside Zip archives will preserve their natural character encoding. To be able to handle these filenames correctly, Web File Share needs to identify the character set and convert it to UTF-8. In order to achieve this you will need to provide some hints on the probable used encoding. You can define a list of encodings inside the "/*path-to-Web File Share*/customizables/config.php" configuration file, like this:

$config['app']['encoding']['detect'] = "ASCII, UTF-8, BIG-5, EUC-CN";*//this is an example that should help detect Chinese encodings*

You can find here "http://www.php.net/manual/en/function.mb-list-encodings.php" the list of encodings that PHP can currently detect.

Note: Most modern programs are using the latest Zip formats and encode the filenames using UTF-8, so there should be no need for any configuration on Web File Share' side.

File Encryption

AES Crypt (http://www.aescrypt.com) is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files. Quik File Share can use it to allow users to encrypt their files. The option is disabled by default. Once "AES Crypt" is installed on your server, follow these steps to enable it inside Quik File Share:

1. Open the file "/*path-to-Quik File Share*customizables/custom_actions/crypt/app.php" in a text editor.
2. Replace the line that

var $disabled = **true**;

with

var $disabled = **false**;

3. Set the path to the "aescript" binary on the line that looks like this:

$pathToAESCrypt = "aescript";

Once it has been enabled, you might need to empty/clear your browser's cache to see the option inside the Quik File Share user interface. To do that, use the CTRL+SHIFT+DELETE keyboard shortcut in your browser.

The feature has been implemented as a "Custom file actions" and it can be easily customized for any other third-party file encryption programs or algorithms.

Hiding file types for certain users or groups

Login as superuser, open the control panel and locate the ID of the group or user you want to configure the filter for. In most browsers, when you keep the cursor over a link, you will see the URL in the browser's status bar. You can use that to easily find the ID of a particular group or user. In most Web File Share control panel URLs, the group ID is marked as "gid" and user ID as "uid".

Open the file "*/path-to-WebFileShare/*customizables/config.php" in a text or PHP editor.

Add the following line inside the file, before its last line ("?>"):

```
 $config['app']['custom_hidden_files']['groups']['123'] = array("*.dwg", "*.DWG", "*.bak", "*.BAK");
```

The above line will hide the file types "dwg" and "bak" from all the users in the group with ID 123.

Please note that the extension is case sensitive, that is why are set twice in the example.

```
$config['app']['custom_hidden_files']['users']['321'] = array("*.ai", "*.AI", "*.dmp", "*.DMP");
```

The above line will hide the file types "ai" and "dmp" from a particular user with the ID 321.

```
$config['app']['custom_hidden_files']['roles']['456'] = array("*.jpg", "*.JPG");
```

The above line will hide the "JPEG" images files from all users with the role ID "456".

You can add as many lines as you need, for different groups and/or users. You can also add as many extensions as you need to a configuration line.

Custom authentication

There are two quick steps (that require PHP knowledge) to set up thirdparty authentication:

1. Define the authentication plugin inside the file "*/path-to-WebFileShare*/customizables/config.php", at line 5. Here's an example for the LDAP authentication:

```
$config['system']['custom_auth_file'] = "auth/ldap.auth.php";
```

2. Use one of the provided authentication plugin files to setup your own:
    1. MySQL: "*/path-to-WebFileShare*/customizables/auth/mysql.auth.php"

3. Joomla: "*/path-to-WebFileShare*/customizables/auth/joomla.auth.php"
    1. Omnisecure: "*/path-to-WebFileShare*/customizables/auth/omnisecure.auth.php"
    2. WordPress: "*/path-to-WebFileShare*/customizables/auth/wordpress.php"
    3. LDAP: "*/path-to-WebFileShare*/customizables/auth/ldap.auth.php"

Before enabling the external authentication, it is recommended to change the Web File Share superuser account's username (default username "admin") to one that matches a username in your external system. This way, when you login to Web File Share with the external credentials you will have superuser privileges.

Joomla authentication

Web File Share can connect to "Joomla CMS" application to share its authentication system. So a Joomla user can access its Web File Share account without entering its username and password again.

Before setting up the plugin, remember to change the username of the Web File Share superuser account, to match an existing Joomla account. This Joomla account will be used to login as Web File Share superuser once the authentication integration is enabled.

Joomla version 1.5.X and higher

1. Define the authentication plugin file ("joomla_v1.5_auth.php") inside the file "*/path-to-Web File Share*/customizables/config.php", at line 5, like this:

/ Custom Authentication */*

```
$config['system']['custom_auth_file'] = "auth/joomla/joomla_v1.5_auth.php";
```

2. Open "*/path-to-Web File Share*/customizables/joomla_v1.5_auth.php" in a text editor and configure the plugin:

a) Specify the path to your Joomla installation , at line 7:

```
$this->config['joomla']['paths']['root'] = "/path/to/joomla/";
```

b) Define the template used for setting up the users' home folder paths:

```
$this->config['users_home_folder_template'] = "/path/to/{USERNAME}/home/folder/";
```

3. Login to Joomla's administration section and open the "Extension Manager". Use the "Upload Package File" option to upload and install the module file "*/path-to-Web File Share*/customizables/Joomla 1.5.x_Web File Share_Authentication_Integration.zip".

4. Go to Joomla's "Plug-in Manager", filter the list of plugins by "Web File Share" and click the plugin "User - Web File Share Authentication Integration". Use the form to enable the plugin. No other changes are needed.

Older Joomla versions

1. Define the authentication plugin file ("joomla.auth.php") inside the file "*/path-to-Web File Share*/customizables/config.php", at line 5, like this:

/ Custom Authentication */*

```
$config['system']['custom_auth_file'] = "auth/joomla/joomla.auth.php";
```

2. Open "*/path-to-Web File Share*/customizables/joomla.auth.php" in a text editor and configure the plugin:

a) Specify the path to your Joomla installation, at line ~31:

```
$this->config['joomla']['paths']['root'] = "/path/to/joomla/";
```

b) Define the template used for setting up the users' home folder paths, at line ~142:

```
"homefolder" => str_replace("{USERNAME}", $username, $users_home_folder_template),
```

Wordpress authentication

This quick guide will help you configure Web File Share to authenticate the users against the database of an existing Wordpress (http://wordpress.org) installation.

It has been tested with Wordpress version 3.0.1.

Download plugins

Download the file "http://www.WebFileShare.com/downloads/WebFileShare_Wordpress_Login.zip" to your computer.

Install the Wordpress plugin

This plugin is needed for allowing the logged in Wordpress users to access Web File Share without having to login twice.

1. Upload the file "WebFileShare-sso.php" inside the folder "/path-to-wordpress/wp-content/plugins/".
2. Login to Wordpress as admin, select "Plugins" from the menu and activate the plugin named "Web File Share Single Sign-On"

Install the Web File Share plugin

1. Open the file "/path-to-WebFileShare/customizables/config.php" in a text editor and change the line #5 like this:

$config['system']['custom_auth_file'] = "auth/wordpress.php";

Configure the Web File Share plugin

Open the file "/path-to-WebFileShare/customizables/auth/wordpress.php" in a text editor and set the path to your Wordpress installation folder, at line #9:

$this->config['wordpress']['path']['root'] = "/www/wordpress";

Please make sure the path uses only forward slashes, even if you are running a Windows server. Inside this file you can also change the default options and permissions of the Web File Share users.

Testing

You should now be able to login to Web File Share, using Wordpress credentials. To login with Web File Share superuser permissions, use a Wordpress account that has the same username as the Web File Share superuser (default username "admin").

Translating Web File Share

Editing a translation

Select a language by clicking on its name. The translation is split in several parts which refer to particular sections or features of Web File Share.

Click the section you wish to edit and you will see a list of words and phrases.

Simply click the text you wish to edit. Each Web File Share client can maintain its own version of the translations. On the third column of the table you can see the translations of the other clients, including the default translation if one is available. Please note that all the translations are public, so it is best to avoid writing information that you would like to keep private.

After you are done editing, you can download your version of the translation by returning to the page listing the sections and clicking the “Download language file” link. You will get a file named “LanguageName.txt” that you can apply to your Web File Share installation.

The language file can be either uploaded by FTP inside “system/data/languages” folder or through Web File Share's control panel, under “System Configuration > Interface options” page.

Note: If you are uploading a translation file via FTP and the translation does not work, make sure your FTP program isn't altering the file's contents (the line endings).

Translating e-mail notifications

The following e-mail message templates can also have translations: “account_notification.tpl.txt”, “forgot_password.tpl.txt”, “reset_password.tpl.txt”, “signup_email.tpl.txt”, “space_quota_warning.tpl.txt”.

To add a translation create a folder named “language-name” inside “customizables/emails/” and make copies of the template files that you want to customize. This system can also be used for customizing the templates while preventing software updates from overwriting your customization.

The main notification template, which is editable through the control panel, can also have translations. Simply copy the template from the control panel into a file named “notifications.tpl.txt” and place inside “customizables/emails/language-name/”. Make sure it has a <Subject> and <Body> tags as the template file “account_notification.tpl.txt” has.

Manually editing a translation file

- The lines begging with “+–” should not be modified as they represent the section name (Example: “+– Login Page –+”)
- The lines beginning with “//” represent comments, and do not require translation.
- Each translated phrase require 2 consecutive lines, the first line is the key and should not be altered in any way. The second line represents the translation.
- The translation should not contain more than one line: the line should not be broken by pressing the “ENTER” key.
- Each phrase translation and section name should be separated by an empty line. Please make sure you don’t leave any blank characters on the separation line, and you do not separate with more than one line.
- If a key is missing from the translation file, the default English version of that text will be displayed.

The API

Quick start for PHP developers

1. Read the Authorization section bellow to understand the requirements.
2. Follow “a new client application”
3. Download and use the Web File Share PHP API Client library:https://github.com/WebFileShare/api-client

Authorization

The WebFileShare API uses the OAuth 2.0 protocol for authentication and authorization.

If you are new to OAuth2, here you can find a good article about it
here: https://aaronparecki.com/articles/2012/07/29/1/oauth2-simplified

Important note: To use the WebFileShare API, your webserver needs to be configured with a SSL certificate. The URL of the Web File Share installation needs to start with HTTPS. Unsecured HTTP connections will be refused, as it represents a serious security vulnerability. Get a free SSL certificate here: https://letsencrypt.org

Testing without SSL

Adding the following line inside /customizables/config.php would allow OAuth2 to be enabled even though you do not access the Web File Share installation via HTTPS:

$config['app']['api']['oauth2']['allow_over_http'] = true;

Warning: This disables the entire security of the API. Your Web File Share users private information will be at risk. Do not use it for production!

Adding a new client application

Before you can start using OAuth2 with your application, you’ll need to tell Web File Share a bit of information about the application. Follow these steps:

1. Login to Web File Share as superuser
2. Open the control panel and navigate to “System configuration” > “Oauth2” > “Clients”
3. Click “Add” and fill in the form
4. Web File Share will generate a “client id” and a “client secret”. Make a note of these two, as you will need to set them in your application.

Obtain an access token

Before your application can access private data using a Web File Share API, it must obtain an access token that grants access to that API. A single access token can grant varying degrees of access to multiple APIs. A variable parameter called “scope” controls the set of resources and operations that an access token permits. During the access-token request, your application sends one or more values in the “scope” parameter.

There are several ways to make this request, and they vary based on the type of application you are building. For example, a web-based application might request an access token using a browser redirect to Web File Share, while an application installed on a device that has no browser uses web service requests.

Some requests require an authentication step where the user logs in with their Web File Share account. After logging in, the user is asked whether they are willing to grant the permissions that your application is requesting. This process is called *user consent*.

If the user grants the permission, the Web File Share Authorization Server sends your application an access token (or an authorization code that your application can use to obtain an access token). If the user does not grant the permission, the server returns an error.

The authorization sequence begins when your application redirects a browser to a specific Web File Share URL; the URL includes query parameters that indicate the type of access being requested.

For web applications

This method is called in OAuth 2.0 terms “the authorization code flow”.

Authentication Endpoint URL: /oauth2/authorize/

The set of query string parameters supported by the Web File Share Authorization Server for web server applications are:

Parameter	Value	Description
response_type	code	Determines whether the Web File Share OAuth 2.0 endpoint returns an authorization code. Web server applications should use code.
client_id	The “client id” you obtain from the Web File Share control panel	Identifies the client that is making the request. The value passed in this parameter must exactly match the value shown in the Web File Share Control Panel
redirect_uri	One of the “redirect uri” values listed for this application	Determines where the response is sent. The value of this parameter must exactly match one of the values listed for your application in the Web File Share control panel, including the http or https scheme, case, and trailing '/').
scope	Space-delimited set of permissions that the application requests.	Identifies the Web File Share API access type that your application is requesting.
state	Any string	Provides any state that might be useful to your application upon receipt of the response. The Web File Share Authorization Server roundtrips this parameter, so your application receives the same value it sent. To mitigate against cross-site request forgery (CSRF), it is strongly recommended to include an anti-forgery token in the state, and confirm it in the response.

An example request URL is shown below, with line breaks for readability.

```
https://www.your-site.com/WebFileShare/oauth2/authorize/?
  scope=email%20profile&
  state=SOME-RANDOM-DATA&
  redirect_uri=https%3A%2F%2Fwww.your-app.com%2Fdo-something-with-the-code&
  response_type=code&
  client_id=f9c6f82cb3e872a20e6a310f33a9c450
```

You web application will be redirecting the users to a similar URL. Web File Share then handles the user authentication and consent. The result is an authorization code, which your application can exchange for an “access token” and a “refresh token”.

Handling the response

The response will be sent to the “redirect_uri” as specified in the request URL. If the user approves the access request, then the response contains an authorization code and the state parameter (if included in the request). If the user does not approve the request, the response contains an error message.

Important: if your response endpoint renders an HTML page, any resources on that page will be able to see the authorization code in the URL. Scripts can read the URL directly, and all resources may be sent the URL in the Referer HTTP header. Carefully consider if you want to send authorization credentials to all resources on that page (especially third-party scripts such as social plugins and analytics). To avoid this issue, we recommend that the server first handle the request, then redirect to another URL that doesn't include the response parameters.

Getting the access token

After your web application receives the authorization code, it should exchange it for an access token and a refresh token, by making an HTTP POST request to the following URL:

Token Endpoint URL: /oauth2/token/

Parameters:

Parameter	**Description**
code	The authorization code returned from the initial request.
client_id	The “client id” obtained from the Web File Share control panel
client_secret	The client secret obtained from the Web File Share control panel.
redirect_uri	One of the redirect URIs listed for this project in the
grant_type	As defined in the OAuth 2.0 specification, this field must contain a value of “authorization_code”.

A successful response to a request contains the following fields:

Parameter	Description
access_token	The token that needs to be sent to the Web File Share API for a regular request.
refresh_token	A token that may be used to obtain a new access token. Refresh tokens expire in 30 days.
expires_in	The remaining lifetime of the access token. Access tokens expire in 60 minutes.
token_type	Identifies the type of token returned. At this time, this field will always have the value Bearer.

Here's how an example response looks like:

```
{
"access_token":"PJIeg5uIs31JBmTGmcUFap6Gv2xhJQs84IqetJeL",
"token_type":"Bearer",
"expires_in":3600,
"refresh_token":"Sj5267kclpjhrvT0pdcE8mVbYxoZTu3u8flqg5cY"
}
```

The application should store the refresh token for future use and use the access token to access the Web File Share API. Once the access token expires, the application uses the refresh token to obtain a new one.

For installed applications

This method is called in OAuth 2.0 terms the “resource owner credentials flow”. It is also known as the “password” flow.

Desktop and mobile application, if they cannot redirect the user to the Web File Share URL for authentication and providing consent, they usually just prompt the users for their Web File Share username and password.

The process requires just a direct HTTP POST call to the token endpoint (/oauth2/token/), with the following parameters:

Parameter	Description
username	The Web File Share user account username.
password	The Web File Share user account password.
scope	Space-delimited set of permissions that the application requests. Identifies the Web File Share API access type that your application is requesting. Each API method that your application will be using requires a certain scope. See that further down in the documentation.
client_id	The “client id” obtained from the Web File Share control panel
client_secret	The client secret obtained from the Web File Share control panel.
redirect_uri	One of the redirect URIs listed for this application inside the Web File Share control panel.
grant_type	As defined in the OAuth 2.0 specification, this field must contain a value of “password”.

Please see the above section Getting the access token for handling the response.

Note: This type of authorization is protected against brute force attacks, just as the regular Web File Share login. If yo File Share user account will get deactivated.

Example

```
curl -X POST -d "username=john&password=love123&scope=upload&client_id=WebFileShare00000000000000000000Mobile&client_se
uri=http://localhost&grant_type=password" https://demo.WebFileShare.co/oauth2/token/
```

- `john` and `love123` - are the Web File Share account's username and password
- `WebFileShare00000000000000000000Mobile` - is the the default API client id used by the mobile apps. It is recommend application.
- `0000000000000000NoSecret0000000000000000` - the API client secret
- `http://localhost` - one of the API configured redirect URLs for the particular API client
- `https://demo.WebFileShare.co` - the URL of your WebFileShare installation

Refreshing the access token

As access tokens expire, you will need to get fresh one once in a while. You do that by making a HTTP call to the follo

Refresh Token Endpoint URL: **`/oauth2/token/`**

Parameters:

Parameter	Description
client_id	The “client id” obtained from the Web File Share control panel
client_secret	The client secret obtained from the Web File Share control panel.
grant_type	As defined in the OAuth 2.0 specification, this field must contain a value of “refresh_token”.

Parameter	Description
refresh_token	The refresh token you have received along with the access token.

A successful response to a request will be identical to the response you receive when you are requesting an initial acc

Note: Save refresh tokens in secure long-term storage and continue to use them as long as they remain valid.

Calling the Web File Share API with the access token

After your application obtains an access token, you can use the token to make calls to the Web File Share API on beha
token in a request to the API by including the “Authorization: Bearer” HTTP header.

Example:

```
GET /WebFileShare/api.php/account/info HTTP/1.1
Authorization: Bearer 8vDeNtzJ8Nf1P0fH1YsvIubOMGttXpqOmupl3oD1
Host: www.your-site.com
```

Where “`8vDeNtzJ8Nf1P0fH1YsvIubOMGttXpqOmupl3oD1`” is the access token received on the previous step.

For most API calls, the server reply will contain a JSON object in the response body. Successful requests will have a pr
For failed requests, the “success” value will be set to “false” and the “error” property will be populated with an textua
supposed to provide information, such as attaching a web link to a file, the property “data” will be populated if the op

Access tokens are valid only for the set of operations and resources described in the scope of the token request. For e
listing directory contents (scope=list), it cannot be used for accessing the user's profile information (scope=profile). Y
WebFileShare API multiple times for similar operations.

Access tokens have limited lifetimes (around 1 hour). If your application needs access to the Web File Share API beyo
obtained refresh token to get a new access token.

API methods

Getting user account information

Target URL	**`/api.php/account/info`**
Required scope	profile
HTTP Method	GET/POST
Output format	JSON

Retrieving lists of files and folders

Target URL	**`/api.php/files/browse/`**
Required scope	list
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Default value	Required	Description

Parameter	Type	Default value	Required	Description
path	string		Yes	Examples: /ROOT - shows a list with items like “My Files”, “Shared with me”, “Starred” (the lis future) / - same as above /ROOT/HOME - items located inside the users home folder (My Files) /STARRED - starred items /PHOTOS - latest photos /MUSIC - latest audio files /SHARES - items shared by the user /LINKS - items shared through web links /ROOT/SHARED - users with shares or folders shared anonymously by other users /ROOT/123 - lists folders shared by user with ID 123. /ROOT/123/456 - list items inside the share with ID 456 owned by user with ID 123.
itemType	string		Yes	Choose type of items to list. Possible values: any - lists both files and folders files - lists only files folders - lists only folders
recursive	boolean	false	No	List items from all the subfolders.
details	array		No	Allows you to choose what information should be retrieved for each file.
details[uuid]	array key		No	unique id which can be used for referencing the file or folder
details[mdate]	array key		No	modified date
details[mdateHuman]	array key		No	modified date in a friendly format
details[cdate]	array key		No	creation date
details[hasWebLink]	array key		No	if file has weblink attached to it or not
details[weblink]	array key		No	retrieve weblink URL
details[weblink-full]	array key		No	retrieve full weblink details
details[description]	array key		No	file type description
details[ext]	array key		No	file extension
details[type]	array key		No	type of file (defined inside system/data/filetypes.php)
details[icon]	array key		No	filename of the Web File Share icon associated with this type of files
details[hasThumb]	array key		No	shows if Web File Share can generate a thumbnail for the file
details[fileSize]	array key		No	includes the file size in bytes
details[nicerFileSize]	array key		No	includes formatted file size
details[commentsCount]	array key		No	includes number of attached user comments
details[label]	array key		No	includes files labels
details[isLocked]	array key		No	shows if file is locked
details[version]	array key		No	includes current file version
details[isShared]	array key		No	shows if folder is currently shared

Example

Listing only files from the users home folder, retrieving information about their attached weblinks and also including a

```
path=/ROOT/HOME
itemType=files
details[[]]=nicerFileSize
details[[]]=weblink
```

path=/ROOT/HOME - the users home folder

itemType=files - listing only files

details[]=nicerFileSize - including a formatted filesize

details[]=weblink - including the URL, if a weblink is attached

Expected output:


```
{
  "success":true,
  "error":false,
  "data":{
    "meta":{
      "path":"\/ROOT\/HOME",
      "parentPath":"\/ROOT",
      "folderName":"Home Folder",
      "perms":{
        "upload":true,
        "download":"1",
        "alter":true
      }
    },
    "files":[
      {
        "filename":"WebFileShare_Admin_Guide.pdf",
        "weblink":"http:\/\/demo.WebFileShare.com\/wl\/?id=89M",
        "is_dir":false,
        "nicerFileSize":"123 KB"
      },
      {
        "filename":"WebFileShare_License_Agreement.pdf",
        "is_dir":false,
        "nicerFileSize":"116 KB"
      },
      {
        "filename":"WebFileShare_User_Guide.pdf",
        "is_dir":false,
        "nicerFileSize":"195 KB"
      },
      {
        "filename":"Welcome.jpg",
        "is_dir":false,
        "nicerFileSize":"17 KB"
      }
    ]
  }
}
```


Retrieving metadata

Target URL	**/api.php/files/metadata/**
Required scope	metadata
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Default value	Required	Description
path	string		Yes	Examples: /ROOT/HOME/file.ext - retrieves metadata for a file named `file.ext` available in the Wel folder

Searching files and folders by name

Target URL	**`/api.php/files/search/`**
Required scope	list
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Default value	Required	Description
path	string		Yes	Path relative to the user's home folder.
keyword	string		Yes	The keyword to search the file names for.
details	array		No	The same as as for the task above.

Creating folders

Target URL	**`/api.php/files/createfolder/`**
Required scope	upload
HTTP Method	POST/GET

Request Parameters Reference

Parameter	Type	Description
path	string	Web File Share path of the new folder's parent.
name	string	Name of the new folder.

Uploading files

Target URL	**`/api.php/files/upload/`**
Required scope	upload
HTTP Method	PUT
Output format	JSON

Request Parameters Reference

Parameter	Type	Description

Parameter	Type	Description
path	string	The Web File Share path of the target file.

Example

```
curl -X PUT --header "Authorization: Bearer neY6uAjKO1KqQh98RZZ5DOgYjIPMuu9duvvHGUiN" -T your-file.ext https://demo.WebFileSha
my-file.ext
```

- `neY6uAjKO1KqQh98RZZ5DOgYjIPMuu9duvvHGUiN` - is the previously received “access_token”
- `your-file.ext` - is the path of the file you want to upload from the local computer
- `https://demo.WebFileShare.co` - is the URL of your Web File Share installation
- `/ROOT/HOME/make-new-folder/my-file.ext` - is the remote path where you wish the file to be uploaded. Web File Share already exist.

Downloading files

Target URL	**/api.php/files/download/**
Required scope	download
HTTP Method	GET/POST
Output format	HTTP DOWNLOAD

Request Parameters Reference

Parameter	Type	Description
path	string	The Web File Share path of the file.

Downloading thumbnails

Target URL	**/api.php/files/thumbnail/**
Required scope	download
HTTP Method	GET/POST
Output format	HTTP DOWNLOAD

Request Parameters Reference

Parameter	Type	Description
path	string	The Web File Share path of the file.

Renaming files or folders

Target URL	**/api.php/files/rename/**
Required scope	modify

HTTP Method	GET/POST
Output format	HTTP DOWNLOAD

Request Parameters Reference

Parameter	Type	Description
path	string	
newName	The new file/folder name.	

Deleting files or folders

Target URL	**/api.php/files/delete/**
Required scope	delete
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Description
path	string	The Web File Share path of the target file.
permanent	boolean (1/0)	Either the file should be permanently removed, instead of just moved to the trash folder.

Starring files or folders

Target URL (add)	**/api.php/files/star/**
Target URL (remove)	**/api.php/files/unstar/**
Required scope	modify
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Description
path	string	The Web File Share path of the target file/folder.

Create web links on files and folders

Target URL	**/api.php/files/weblink/**
Required scope	weblink

HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Description
path	string	The Web File Share path of the target file/folder.
singleDownload	boolean	Returns a link which is valid for a single download. This does not affect web links the user might have previously created file/folder.
temporary	boolean	Returns a link which is valid for 15 minutes. This does not affect web links the user might have previously created on the

Example reply:

```
{
  "success": true,
  "error": false,
  "data": {
    "status": "created", //can also return "existing"
    "url": "http:\/\/www.yoursite.com\/WebFileShare\/wl\/?id=CtmsT8lWoen3JDZlVbxvR3SH45gvvvxs",
    "isdir": false //or true if you are linking a folder
  }
}
```

Sharing folders

Target URL	**/api.php/files/share/**
Required scope	share
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Required	Description
path	string	Yes	The Web File Share path of the folder.
uid	integer	Yes if no “gid”	ID of Web File Share user to share folder with.
gid	integer	Yes if no “uid”	ID of Web File Share group to share folder with.
anonymous	boolean	No	Specify if folder is to be shared anonymously.
upload	boolean	No	Specify if upload permission is granted.
download	boolean	No	Specify if download permission is granted.
comment	boolean	No	Specify if the permission to post comments is granted.
read_comments	boolean	No	Specify if the permission to read comments is granted.
alter	boolean	No	Specify if the permission to make file changes is granted.
share	boolean	No	Specify if the permission to share files is granted.
alias	string	No	Specify an alias for the shared folder name.

Note: If the folder was already shared, the share settings will be updated. No errors will be returned in that case.

Unsharing folders

Target URL	**/api.php/files/unshare/**
Required scope	share
HTTP Method	GET/POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Required	Description
path	string	Yes	The Web File Share path of the folder.
uid	integer	Yes if no “gid”	ID of Web File Share user to be removed from the share.
gid	integer	Yes if no “uid”	ID of Web File Share group to be removed from the share.

Note that the call will return an error if the folder is not shared with the specified user or group.

Get Web File Share user account information

Target URL	**/api.php/admin-users/info**
Required scope	admin
HTTP Method	POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Required	Description
UID	integer	Yes, if `uname` not provided	User ID
uname	string	Yes, if `UID` not provided	Username

Add Web File Share user accounts

Target URL	**/api.php/admin-users/add**
Required scope	admin
HTTP Method	POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Default value	Required	Description

Parameter	Type	Default value	Required	Description
generate_password	boolean		No	Set to 1 to have Web File Share assign a randomly generated password
create_home_folder	boolean		No	Set to 1 to have Web File Share create the user's home folder if it doesn
data[username]	string		Yes	The username may not contain special characters, except for underscor
data[name]	string		Yes	
data[password]	string		No	
data[two_step_enabled]	boolean	0	No	
data[two_step_secret]	string		No	
data[last_pass_change]	date	NULL	No	
data[owner]	integer	NULL	No	This can be the ID of the parent independent admin user.
data[registration_date]	date	current date	No	
data[activated]	boolean	1	No	
data[expiration_date]	date	NULL	No	
data[require_password_change]	boolean	0	No	
data[email]	string		No	
data[receive_notifications]	boolean	0	No	
data[company]	string		No	
data[website]	string		No	
data[description]	string		No	
data[logo_url]	string		No	
perms[role]	integer	NULL	No	
perms[admin_type]	string	NULL	No	Possible values: `simple` , `indep`
perms[admin_users]	boolean	0	No	
perms[admin_roles]	boolean	0	No	
perms[admin_notifications]	boolean	0	No	
perms[admin_logs]	boolean	0	No	
perms[admin_metaperms]	boolean	0	No	
perms[admin_over]	mixed		No	Set to “-ALL-” if the user is an admin who can manage all other users
perms[admin_max_users]	boolean	0	No	
perms[admin_homefolder_template]	string		No	
perms[homefolder]	string		Yes	The is an absolute path to a folder existing in the server's file system. A servers.

Parameter	Type	Default value	Required	Description
perms[space_quota_max]	integer	0	No	
perms[space_quota_current]	integer	0	No	
perms[traffic_quota_max]	integer	0	No	
perms[traffic_quota_current]	integer	0	No	
perms[readonly]	boolean	0	No	
perms[upload]	boolean	1	No	
perms[download]	boolean	1	No	
perms[download_folders]	boolean	1	No	
perms[read_comments]	boolean	0	No	
perms[write_comments]	boolean	0	No	
perms[email]	boolean	0	No	
perms[weblink]	boolean	0	No	
perms[share]	boolean	0	No	
perms[btsync]	boolean	0	No	
perms[metaperms]	boolean	0	No	
perms[file_history]	boolean	0	No	
perms[users_may_see]	string	-ALL-	No	
perms[change_pass]	boolean	1	No	
groups	array		No	A list of group names. If groups with the specified names are not found,

Example response

Example response after successful request:

```
{
  "success": true,
  "error": false,
  "data":{
    "generated_password": "12345678",
    "uid": "44"
  }
}
```

Where “44” is the ID of the newly created user account and “12345678” is the password generated by Web File Shar

Example response after failed request:

```
{
  "success": false,
  "error": "The value of data[username] needs to be unique in the database",
  "code": "username_in_use"
}
```


Modify Web File Share user accounts

Target URL	**/api.php/admin-users/edit**
Required scope	admin
HTTP Method	POST
Output format	JSON

Request Parameters Reference

Besides the parameters described higher, for adding user accounts, this API method uses also the following:

Parameter	Type	Required	Description
UID	integer	Yes	The user ID

Delete Web File Share user accounts

Target URL	**/api.php/admin-users/delete**
Required scope	admin
HTTP Method	POST
Output format	JSON

Request Parameters Reference

Parameter	Type	Required	Description
UIDS	array	Yes	Array of user ID integers
deleteHomeFolder	boolean	No	If included, this will cause the user(s) home folders to also be deleted.

Revoking app authorization (for users)

Users can see the authorizations made for the various apps, inside the “Account Settings” and can revoke them from

Troubleshooting

"Check the "access_token" parameter"

If you cannot get past the error *“The request is missing a required parameter, includes an invalid parameter value, in malformed. Check the “access_token” parameter.”*, although you have checked and your HTTP request includes the “ perhaps PHP doesn't get the variable “ `$_SERVER['HTTP_AUTHORIZATION']` ” populated. In which case, if you are running A “ `.htaccess` ” file:

```
RewriteEngine On
RewriteCond %{HTTP:Authorization} .+
RewriteRule .* - [[E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]]
```

If you are using a virtual host, make sure the above is inside the Virtualhost tag, not in Directory tag.

Table of Contents

- **The API**
  - Quick start for PHP developers
  - Authorization
    - Testing without SSL
    - Adding a new client application
    - Obtain an access token
    - Refreshing the access token
  - Calling the FileRun API with the access token
  - API methods
    - Getting user account information
    - Retrieving lists of files and folders
    - Retrieving metadata
    - Searching files and folders by name
    - Creating folders
    - Uploading files
    - Downloading files
    - Downloading thumbnails
    - Renaming files or folders
    - Deleting files or folders
    - Starring files or folders
    - Create web links on files and folders
    - Sharing folders
    - Unsharing folders
    - Get FileRun user account information
    - Add FileRun user accounts

Running custom scripts when users perform various actions

Custom PHP scripts can be automatically executed when the users perform one of the 57 monitored actions (E-mail_notification_system#Actions_keynames).

For example, to automatically run custom PHP code whenever a file is uploaded, you can simply place a PHP file named "upload.php" inside the folder "/*path-to-WebFileShare*/customizables/events/"

Here's a list of useful scripts:

Set file permissions after upload:

```
$data = unserialize($data['data']);

chmod($data['full_path'], 0644);
```

Antivirus check on upload:

```
<?php

global $auth;

$data = unserialize($data['data']);

$info = array(

                "username" => $auth->currentUserInfo['username'],

                "fullPath" => $data['full_path']

);



$pathToShellScript = "virus_scan.sh";

//virus_scan.sh will be executed with the username and the file's path

@system($pathToShellScript." ".escapeshellarg($info['username'])." ".escapeshellarg($info['fullPath']);
```

Filter uploaded files by extension:

```
<?php

$extensions = array("exe", "dll"); //customize the list of banned extensions

/*************************************************************/

global $fm;

$data = unserialize($data['data']);
```

```
$ext = $fm->getExtension($data['filename']);

if (in_array($ext, $extensions)) {

                unlink($data['full_path']);

}
```

Counting file downloads

Applies to Web File Share version (260213)

To keep track of the files' download count, please follow these steps:

- Login as superuser and open the Control Panel
- Select "System configuration » Metadata » Fieldsets" and click "Add"
- Set the "Field set name" (Something like "Info", it doesn't really matter)
- Enable the "Generic field set" option (So that all files show this field set)
- Click "Add Field Set"
- Activate the "Field sets" tab and double-click in the list the newly created field set
- Inside the "Fields" section, click "Add".
- Type "Downloads" for the "Field name" and click "Save".
- You need the ID of the recently added field. You can get that directly from the MySQL database, by browsing the table "df_modules_metadata_fields"
- Create the text file "*/path-to-WebFileShare/*customizables/events/download.php" and paste the following code inside:

```
<?php



$fieldId = XXXX; //set here the ID of the metadata field that will be holding the downloads count



/*-------------------------------------------------------------------*/



global $metadata, $db;

$data = unserialize($data['data']);

$metaFileInfo = $metadata->files->getByPath("*", $data['full_path']);//get file metadata record



if (!$metaFileInfo['id']) {

                $id = $metadata->files->addFile($data['full_path']);//add file metadata record if not found

                if ($id) {

                                $metaFileInfo['path'] = $data['full_path'];

                                $metaFileInfo['id'] = $id;

                }

}



$rs = $metadata->get($metaFileInfo['id'], array($fieldId));//get current download count



$downloads = $rs[0]['val'];

if (!$downloads) {
```

```
                $downloads = 0;

}

$metadata->set($metaFileInfo['id'], $fieldId, $downloads+1);//increment the download count
```

- Replace the "XXXX" with the ID of your "Downloads" metadata field on the first line of the script file.

The "download.php" script will execute each time a user downloads a file, and it will increment the value it finds in the file's "Downloads" metadata field. You can reset the count at any time, by editing the value from the Metadata menu.

Being a metadata field, you can also display it as a column in the file list view, to have a quick view over how many time the files were downloaded.

File reference

DEV Files

This is a list of most customized Web File Share files and folders:

```
/css/style.css
```

The CSS file that needs to be edited for changing the background for the login page.

```
/customizables/include.html
```

It can be used to include HTML code inside the login page and on the main user interface. Can be used for including Google Adwords tracking code.

```
/customizables/config.php
```

This is where configuration directives can be set. A list with the available directives can be found here.

```
/customizables/custom_actions/
```

Contains the plugins responsible with the functionality available under the "Open with.." contextual menu option. The subfolders can be safely removed, if you wish to disable any of the options. For more information about the plugins, click here.

```
/viewers/ and /viewers_mobile/
```

Includes the code that generates the file previews (for both the normal and mobile user interface).

```
/system/data/default_home_folder/
```

This is the superuser's default home folder. It is recommended that you change the location of the Web File Share users' home folders outside the public area of your webserver (ie. outside "public_html" or "www").

```
/system/data/languages/
```

Contains the translation files.

```
/system/data/autoconfig.php
```

Contains the MySQL connection information. This file needs editing if the connection changes (for example when the password gets updated).

```
/system/modules/weblinks/sections/default/html/pages/download.html
```

Displays information about a file before being downloaded through a WebLink.

```
/system/modules/weblinks/sections/default/html/pages/folder.html
```

Displays the list of files for a WebLinked folder.

```
/system/modules/weblinks/sections/default/html/pages/folder_gallery.html
```

Displayed the image gallery for a WebLinked folder.

```
/system/modules/weblinks/sections/default/html/pages/folder_rss.html
```

Generates the XML-formatted RSS feed for a WebLinked folder.

```
/system/modules/weblinks/sections/default/html/pages/invalid_link.html
```

Displays a message to visitors accessing invalid or expired WebLinks.

```
/system/modules/weblinks/sections/default/html/pages/password.html
```

Displays the password form for password-

protected WebLinks.

```
/system/modules/weblinks/sections/default/html/pages/traffic_limit.html
```

Displays the warning when trying to download a file through a WebLink created by a Web File Share user who's traffic quota has been reached.

Adding custom functionality

Custom Modules

This page provides some details on how to add a custom PHP script to Web File Share's framework. The benefits are that the page can be protected by Web File Share's authentication system and that your script can use Web File Share's API. The API has no public documentation, but if you contact us, we'll help you with the required information.

Creating a custom module

To create a module, simply start by creating a new folder "MyModule" (or a name of your choice) inside "*/path-to-Web File Share*/system/modules/".

This module can be accessed using the following URL: **http://your-site/WebFileShare/?module=MyModule**

The above URL will run the file "*/path-to-WebFileShare*/system/modules/MyModule/sections/default/php/default.php".

Each module is split in **sections**, so create a folder named "sections" inside "*/path-to-WebFileShare*/system/modules/MyModule/".

You can specify a section like this: **http://your-site/WebFileShare/?module=MyModule&section=MySection**

The above URL will run the file "*/path-to-Web File Share*/system/modules/MyModule/sections/MySection/php/default.php".

Each section can have multiple **pages**. To call a different script file than "default.php", you can specify a page like this: **http://your-site/WebFileShare/?module=MyModule&section=MySection&page=MyPage**

The above URL will run the file "*/path-to-WebFileShare*/system/modules/MyModule/sections/MySection/php/MyPage.php".

Inside "MyPage.php" you can execute any PHP code you wish to.

Password protecting the pages

Inside "*/path-to-WebFileShare*/system/modules/MyModule/", create a file named "config.php".

Pasting the following code inside, will allow only authenticated users to access the page "MyPage" ("*/path-to-WebFileShare*/system/modules/MyModule/sections/MySection/php/MyPage.php").

```
<?php

$config['modules'][$moduleName]['sections']['MySection']['perms'] = array(

                'MyPage' => array('must_be_logged' => true)

);
```

(Make sure you don't include in the file any space character before the "<?php " part.)

You can protect as many pages as you want. Simply add more items to the above Array.

Forcing certain file types to download

When accessing files via WebLinks, if possible, the browser will try to open the file itself, instead of asking the user to save the file. Common file types, like images or text files will automatically open in the browser. You can force the browser to prompt the user for saving the file, instead of letting it automatically open.

Simply open the file "/*path-to-WebFileShare*/customizables/config.php" in a text editor and add the following line:

```
$config['app']['weblinks']['force_download'] = array("txt", "jpg");
```

You can replace "txt" and "jpg" with the file extension you want and also add more extensions.

Custom file actions

You can easily add custom options inside the "Open with.." file contextual menu. Here is a step by step guide:

1. Make a copy of "*/path-to-WebFileShare/*customizables/custom_actions/_example" inside the same folder and rename it to "*my-action*" (you are free to name the folder as you wish). (Writing an underscore in front of the folder's name disables the option.)
2. Open the file "*my-action*/app.php" in a PHP editor:

- Rename the class to "custom_*my-action*". (Note that this depends on the folder's name.)
- Edit the code according to your requirements:

Define the text that will be displayed for the contextual menu option:

```
$this->JSconfig['title']
```

Define the URL of the contextual menu option's icon:

```
$this->JSconfig['icon']
```

Make the option open a popup window with the specified size.

```
$
```

```
);
```

When using a popup window, the output of the method "custom_*my-action*::run()" will be displayed inside the popup. The "$this->data" array can be used to find the file's path:

```
function run() {

 echo $this->data['filePath'];

}
```

If you wish to execute a JavaScript function (perhaps making an Ajax call) instead of opening a popup, use this instead:

```
$this->JSconfig['fn'] = "alert('Option clicked!')";
```

Add the following option to display the contextual option only for certain filetypes:

```
  $this->JSconfig['extensions'] => array("txt", "pdf", "doc");
```

Allow only users with download permissions to see and use this plugin:

```
  $this->JSconfig['requiredUserPerms'] => array("download");
```

Misc custom actions:

- View Office files with Microsoft Office Web Viewer (download)
- View PDFs and annotate with Crocodoc.com (download)
- View documents online with Vuzit.com (download)

Calculating MD5 Checksums

Hash Files

To automatically calculate and store the files' MD5 checksum values, so you can verify their integrity, please follow these steps:

- Go to "Control Panel » System configuration » Metadata » Fieldsets » Create new"
- Set the "Fieldset name" (Something like "Info", it doesn't really matter)
- Tick the "Generic fieldset" checkbox. (So that all files show this fieldset)
- Click "Save" to add the fieldset.
- Click "Manage Fields > Create new"
- Type "Checksum" for the "Field name" and click "Save"
- By holding the mouse cursor over the newly created field name you can find out its ID, from the link's URL (.....&fid=X)
- Create the text file "*/path-to-WebFileShare*/customizables/events/upload.php" and paste the following code inside:
- Replace the "XXXX" with the ID of your "Checksum" metadata field on the first line of the script file.

The "upload.php" script will execute each time a user uploads a file, and it will calculate the file's hash and store it in the file's "Hash" metadata field.

Being a metadata field, you can also display it as a column in the file list view.

Please note that with this method, PHP reads the entire file's contents into memory. This can be slow and might not even work for files larger than PHP's configured "memory_limit" value.

A solution available for Unix type of servers is to replace the line "

```
$hash = md5(file_get_contents($data['full_path']));
```

", with the following one:

```
$hash = exec("md5sum "".escapeshellcmd($data['full_path'])."""");
```

Adding links to the menu

Applies to Web File Share version (291210)

The menus are defined inside the file "*/path-to-WebFileShare/*js/fileman/toolbars_and_menus.js".

To add a link on the main toolbar (next to the "Upload" and "File" options), you open the file in a text editor and add the following code after the line #185:

```
tbar.push('-');

tbar.push({

 text: FR.T('Your button'), scale: 'medium',

 icon: FR.iconsURL+'/the_icon.gif',

 handler: function() {

   document.location.href = 'http://www.google.com';

 }

});
```

- The button's text can be set by replacing the text "Your button".
- To change the target URL, replace in the above code "http://www.google.com" with your own address.
- To set the icon, place a file named "the_icon.gif" inside "*/path-to-WebFileShare/*images/fileman/interface/icons/". If you don't want an icon for the button, simply delete the line that starts with "icon:".

If you want the button to open the page into a window, replace the line

```
document.location.href = 'http://www.google.com';
```

with the following code:

```
  FR.UI.popup({

      src: 'http://www.google.com/?',

      width: 680, height: 540, constrain: true, maximizable: true, autoDestroy: true

  });
```

Please note that this function automatically adds some variables to the specified URL. To avoid troubles, try ending your URL with a question mark (?) character.

Custom even scripts

Custom PHP scripts can be automatically executed when the users perform one of the monitored actions (Actions_keynames).

For example, to automatically run custom PHP code after a file is uploaded, you can simply place a PHP file named “upload.php” inside the folder “customizables/events/”.

Here's an example script:

Set file permissions after upload:

```
<?php
$data = unserialize($data['data']);
chmod($data['full_path'], 0644);
```

If you want the code to be executed before the file is saved to the folder, so that you can process it and perhaps reject the uploaded file, you need to name the script file “file.upload.php”.

Here's how an example script would look like in this case:

Clamscan antivirus check on upload:

```
<?php
global $auth;
$data = unserialize($data['data']);
$out = '';
$int = -1;
exec($command, $out, $int);
exec("clamscan ".escapeshellarg($data['full_path']), $out, $int);
if ($int != 0) {
return array(
 'error' => array('code' => 100, 'msg' => 'This file has been rejected as it contains viruses!'),
 'return' => false
);
}
```

Prevent non-admin users to delete files labeled as APPROVED.

Place the following code inside “customizables/events/file.delete.php”:

```
<?php
global $auth;
if (!\WebFileShare\Perms::isSuperUser() && !\WebFileShare\Perms::isSimpleAdmin() && !\WebFileShare\Perms::isIndependentAdmin()) {
 $metaFileInfo = \WebFileShare\MetaFiles::getByPath("*", $extra['filePath']);
 if ($metaFileInfo['id']) {
  $label = \WebFileShare\Labels::getByFileId($metaFileInfo['id']);
  $v = \WebFileShare\Labels::parseValue($label);
  if (strtoupper($v['text']) == 'APPROVED') {
   return array(
    'error' => array('code' => 100, 'msg' => 'Approved files cannot be deleted!'),
    'return' => false
   );
  }
 }
}
```

For running a script when folders are being deleted the file needs to be named “folder.delete.php”. To run a script when files are being downloaded, name the script file “file.download.php”.

Calculate and store the files' MD5 checksum values in a metadata field

Please follow these steps:

- Go to “Control Panel » System configuration » Metadata » Fieldsets » Create new”
- Set the “Fieldset name” (Something like “Info”, it doesn't really matter)
- Tick the “Generic fieldset” checkbox. (So that all files show this fieldset)
- Click “Save” to add the fieldset.
- Click “Manage Fields > Create new”
- Type “Checksum” for the “Field name” and click “Save”
- By holding the mouse cursor over the newly created field name you can find out its ID, from the link's URL (……&fid=X)
- Create the text file “customizables/events/upload.php” and paste the following code inside:

```
<?php
```

```
$fieldId = 15; //set here the ID of the metadata field that will be hold the filename

/*-------------------------------------------------------------------------*/

global $db, $fm;
$data = unserialize($data['data']);
$metaFileInfo = \WebFileShare\MetaFiles::getByPath("*", $data['full_path']);//get file metadata record

if (!$metaFileInfo['id']) {
 $id = \WebFileShare\MetaFiles::addFile($data['full_path']);//add file metadata record if not found
 if ($id) {
  $metaFileInfo['path'] = $data['full_path'];
  $metaFileInfo['id'] = $id;
 }
}

$hash = md5(file_get_contents($data['full_path']));

\WebFileShare\MetaValues::set($metaFileInfo['id'], $fieldId, $hash);//set hash as metadata
```

* Replace the “XXXX” with the ID of your “Checksum” metadata field on the first line of the script file.

The “upload.php” script will execute each time a user uploads a file, and it will calculate the file's hash and store it in the file's “Hash” metadata field.

Being a metadata field, you can also display it as a column in the file list view.

Please note that with this method, PHP reads the entire file's contents into memory. This can be slow and might not even work for files larger than PHP's configured “memory_limit” value. A solution available for Unix type of servers is to replace the line “$hash = md5(file_get_contents($data['full_path']));”, with the following one:

```
$hash = exec("md5sum \"".escapeshellcmd($data['full_path'])."\"");
```

External Login Form

The following is a PHP code snippet that displays a login form which provides feedback without showing the Web File Share login screen. This can be used if you would like to have a custom login form integrated into your website and bypass the Web File Share login screen.

```
<?php
if ($_GET[['feedback']]) {
     echo base64_decode($_GET[['feedback']]);
}
?>
<form method="post" action="URL-OF-WebFileShare/?action=login&nonajax=1">
 <input type="hidden" name="redirectAfterLogin" value="<?php echo base64_encode("URL-OF-FILERUN-OR-WELCOME-PAGE")
?>">
 <input type="hidden" name="redirectOnFailure" value="<?php echo base64_encode("URL-OF-PAGE-HOSTING-THIS-FORM?")
?>">
 <label for="usr">Username:</label>
 <input type="text" name="username" value="" id="usr"/>
 <label for="pass">Password:</label>
 <input type="password" name="password" value="" id="pass" />
 <input type="submit" value="Login">
</form>
```

You will need to replace the following placeholders: URL-OF-WebFileShare, URL-OF-PAGE-HOSTING-THIS-FORM (leave the question mark at its end) and URL-OF-WebFileShare-OR-WELCOME-PAGE.

You can also make the login Ajax-based, in which case the HTTP request is identical, but the target URL should not contain the “&nonajax=1” part. The server response will then be in JSON format.

Hiding options from the "Open with..." menu

The options that are displayed in the "Open with..." menu are called "custom actions". Each custom action has a folder inside "/*path-to-WebFileShare*/customizables/custom_actions/". If you want to disable a particular option, you can do that by opening its "app.php" file in a text editor and adding the following line of code;

```
var $disabled = true;
```

right after the line of code that reads "class custom_ {" (usually located on line number 5).

For Web File Share versions 121211 or lower, this is the only way to do it:

Simply delete the folder or renaming it to add an underscore character in front of the name. For example, to disable Google Docs Viewer, you would rename the folder "google_docs_viewer" to "_google_docs_viewer". The disadvantage of this method is that it might cause some troubles when installing software updates. Some software updates add improvements to the custom actions and you might need to have to original file structure, for Web File Share to be able to install the update.

If you are not seeing the change, try to clear your browser's cache (delete temporary Internet files).

Automatic Login

If you wish to automatically login visitors to WebFileShare without asking them to fill in the login form, there are two ways:

Using a custom link

http://YOUR-SITE.COM/WebFileShare/?page=login&action=login&nonajax=1&username=USERNAME&password=PASSWORD

Set the session programmatically

Redirect users to a PHP script like this:

```
<?php
//start WebFileShare session
session_name('WebFileShareSID');
session_start();

$username = "admin";

//set logged in username
$_SESSION[['WebFileShare']][['username']] = $username;

echo "You are now logged in as '".$username."'.";
exit();
```

Copy the above code inside a file named “autologin.php” and place it inside the Web File Share installation folder and then just access “http://www.your-site.com/WebFileShare/autologin.php”

Custom "Open with" actions

Creating a custom “Open with..” file contextual menu option:

The plugin folder structure

- Create a new empty folder inside “customizables/custom_actions/”. For this example we'll name it “hello”.
- Create a file “customizables/custom_actions/hello/app.php”

The PHP class

Inside “customizables/custom_actions/hello/app.php”, start with the following example:

```
<?php

class custom_hello {//required class name "custom_<folder-name>"

 var $online = true; //set this to true if the plugin requires Internet connection. it also makes the option show after the plugins that Web F

 var $disabled = false; //you can use this or the method bellow
 function isDisabled() {//optional method for dynamically enabling/disabling this plugin
  return false;
 }

 function init() {//required method
  //contains only configuration data
  //no other functionality here

  $this->JSconfig = array(
   //required
   "title" => self::t("Hello World"),

   "popup" => true, //opens a popup and runs the method run() inside

    //popup styling
    'iconCls' => 'fa fa-fw fa-file-text-o', //CSS class for menu item icon, remove the bellow if using this
    "icon" => 'url/to/icon.png', //image file for menu item icon, remove the above if using this
    "loadingMsg" => self::t('The plugin is loading. Please wait.'),
    "width" => 500,
    "height" => 500,

    "external" => true, //makes the popup an actual browser popup instead of an in-page one

   "ajax" => true, //instead of the popup above, it makes an Ajax call for the run() method


   "multiple" => true, //show menu item also when multiple files are being selected
   "onlyMultiple" => true, //show menu item ONLY when multiple files are being selected

   "folder" => true, //show menu item only for folders

   'extensions' => [
    'pdf' //show only for PDF files
   ],
   'useWith' => [//the above setting takes precedence over this one
    'txt',  //show only for plain text files
    'office', //show only for office files
    'noext' //.. and files without extension
   ],
   "requiredUserPerms" => ["download", "upload"]
  );
 }

 static function t($text) {//utility method for allowing the plugin to be translated to various languages
  $section = 'Custom Actions: Hello World'; //the translation section
  return \WebFileShare\Lang::t($text, $section);
 }

 function run() {//called inside the popup, or by the Ajax request

  \WebFileShare::checkPerms("download");//important security stuff!


  echo 'Hello World!';
  echo '\\';
  echo 'Relative file path: '.$this->data['filePath'];
  echo '\\';
  echo 'Full file path: '.$this->data['fileName'];
  echo '\\';
  echo 'File name: '.$this->data['relativePath'];
  echo '\\';
  echo 'Full path of plugin folder: '.$this->path;
```

```
 //add the action to the user activity log
 \WebFileShare\Log::add(false, "preview", [
  "relative_path" => $this->data['relativePath'],
  "full_path" => $this->data['filePath'],
  "method" => "Hello"
 ]);
 }

 function dummy() {
  //your popup can access this method through the following URL: ?module=custom_actions&action=hello&method=dummy
 }
}
```

Custom CSS

As software updates are replacing Web File Share's files regardless of the fact that they have been customized, there is a way to make CSS modification which will be preserved between software updates. You can specify the URL of an external CSS file which will get loaded. Simply add the following line inside the configuration file (customizables/config.php):

```
$config['app']['ui']['custom_css_url'] = 'http://www.your-site.com/your-file.css';
```

Replace the example URL with your own valid URL.

Resetting the FileRun superuser password

Running the following from the command line should give you a new password:

```
cd cron
cron> php reset_superuser_pass.php your-site.com newpass
```

You will need to replace your-site.com with the actual domain/hostname of your web server. If you do not specify newpass, a random one will be generated and displayed in the command's output.

Backup

Making a backup

This article doesn't cover backing up your user files, but only the Web File Share installation which includes the user settings, WebLink information, metadata, file comments and any other data the Web File Share users might attach to the files and folders.

There are two parts to a complete back up of your Web File Share installation:

1. The MySQL database information
2. The Web File Share application files and folders

1. MySQL

If you are using a hosting service, you most probably have a MySQL database backup option in the hosting control panel. It should help you download an ".sql" file that contains the database' structure and data.

If there isn't a dedicated backup option, there is most probably "phpMyAdmin", which is a tool for managing MySQL databases that you can use to make the backup.

Backup the database using "phpMyAdmin"

1. Log into phpMyAdmin on your server
2. From the main login screen, select 'Databases' (You may not need to do this step)
3. Now click the name of your database - or your FileRun database if you have several databases.
4. Click the 'Export' tab on the top set of tabs.
5. Look at the left box at the top of the Export section. All the tables in the database you selected are in that box. If you have other programs that use the database, then choose only those tables that correspond to your Web File Share install. They will be the ones with that start with "df_".
6. Ensure that the format type is set to SQL.
7. In the SQL section, tick the following boxes:* 'Structure'* 'Add DROP TABLE'* 'Add IF NOT EXISTS'* 'Add AUTO_INCREMENT'* 'Enclose table and field names with backquotes'
8. Tick the DATA section. (The sub-options do not really make much of a difference.)
9. Tick the 'Save as file' option, and leave the template name as is.\\
10. Now click 'Go' and you should be prompted for a file to download. Save the file to your computer. Depending on the database size, this may take a few moments.
11. You have now backed up your database. If you wanted, you could download a backup in each of the compression formats. Your choice. For example: None and "zipped".

Backup the database from the command line

You will need SSH access to the server or direct access to the server's command line prompt.

```
cd /path/to/Web File Share/
Web File Share> mysqldump --add-drop-table -h localhost -u mysqlusername -p databasename -c > Web File Share.backup.sql
```

Replace "mysqlusername" and "databasename" with the actual names. You can find them inside "system/data/autoconfig.php". You will be asked to enter your MySQL password. Type it and hit Enter.

2. Web File Share application files and folders

This is simple as making a duplicate copy of the Web File Share installation folder. You can use any method (FTP, SSH, or the hosting control panel file manager).

ZGL to ionCube

If you are running Web File Share for "Zend Guard Loader" and want to upgrade to PHP 5.4, or simply switch from "Zend Guard Loader" to "ionCube", you will need to replace the Web File Share application files with more appropriate versions.

You can of course download the latest Web File Share version from the client account and install that, but that will mean reconfiguring the user accounts and the settings and loosing the weblinks, shares, file comments, metadata etc.

In order to preserve the current configuration, you need to have a Web File Share installation zip file that matches the version of your current Web File Share installation and which works with "ionCube". If it's not available for download from your Web File Share client account, you can receive an older installation package by contacting us and letting us know your current Web File Share version.

If your Web File Share installation is still running, you can find the its version by appending "?Web File ShareVersion" to its URL. For example: http://demo.WebFileShare.com/?WebFileShareVersion

If your installation is no longer working (due to the server upgrade), run the following SQL command against the MySQL database:

```
SELECT `val` AS 'Web File Share Version' FROM `df_settings` WHERE `var`='currentVersion'
```

to get the Web File Share version. If you do not know how to do that, we can retrieve the version for you, if you contact us and provide us FTP access to your Web File Share installation folder.

Once you have a Web File Share installation zip that works with "ionCube", please follow these steps:

1. Make a backup copy of your existing Web File Share installation folder!
2. Rename the existing Web File Share installation folder (not the backup copy that you made) to "old_WebFileShare_install".
3. Extract the contents of the Web File Share installation zip archive for "ionCube" in a folder named like your original Web File Share installation folder. For this example, let's assume the folder name was "WebFileShare".
4. Delete the default folder "WebFileShare/system/data" and move "old_WebFileShare_install/system/data" inside "WebFileShare/system/" folder to replace the deleted one. Make sure you make no change to the contents of "old_WebFileShare_install", to prevent loosing users documents and settings.
5. Open a browser and make sure Web File Share works the same as it used to work when the server was running with "Zend Guard Loader". If everything is in order, you can delete the folder "old_WebFileShare_install".

Upgrading to PHP 5.4

PHP5.4

If you are running Web File Share on PHP 5.3 with "ionCube", then you can upgrade your server to PHP 5.4 without any additional change.

If you are running any other version, you will need to replace the Web File Share installation with one that works with PHP 5.4.

You can of course download the latest Web File Share version from the client account and install that, but that will mean reconfiguring the user accounts and the settings and loosing the weblinks, shares, file comments, metadata etc.

In order to preserve the current configuration you need to have a Web File Share installation zip file that matches the version of your current Web File Share installation, and which works with PHP 5.4. You can contact us for it.

If your Web File Share installation is still running, you can find its version by appending "?Web File Share Version" to its URL. For example: http://demo.WebFileShare.com/?WebFileShareVersion

If your installation is no longer working (due to the server upgrade), run the following SQL command against the MySQL database:

```
SELECT `val` AS 'Web File Share Version' FROM `df_settings` WHERE `var`='currentVersion'
```

to get the Web File Share version. If you do not know how to do that, we can retrieve the version for you, if you contact us and provide us FTP access to your Web File Share installation folder.

Once you have a Web File Share installation zip for PHP 5.4, please follow these steps:

1. Make a backup copy of your existing WebFileShare installation folder!
2. Rename the existing WebFileShare installation folder (not the backup copy that you made) to "old_WebFileShare_install".
3. Extract the contents of the Web File Share installation zip archive for PHP 5.4 in a folder named like your original Web File Share installation folder. For this example, let's assume the folder name was "WebFileShare".
4. Delete the default folder "WebFileShare/system/data" and move "old_WebFileShare_install/system/data" inside "WebFileShare/system/" folder to replace the deleted one. Make sure you make no change to the contents of "old_Web File Share_install", to prevent loosing users documents and settings.
5. Open a browser and make sure Web File Share works properly. If everything is in order, you can delete the folder "old_WebFileShare_install".

Migrating to another server

Migrating to a new server

There are three components to a Web File Share installation:

- The application files
- The MySQL database
- The user files

The application files

The Web File Share installation folder can simply be moved or copied from one location to another, the root folder can even be safely renamed, as Web File Share doesn't reference it's own files using absolute paths.

The MySQL database

To move the MySQL database to the new server, please follow the official guide: https://dev.mysql.com/doc/refman/5.7/en/copying-databases.html

If the connection information to the new server differs from the old one, you can update it by opening the system/data/autoconfig.php file in a text editor. You can change the MySQL server hostname, username and password from inside this file.

The user files

Web File Share is referencing files by their full paths in the server's file system. If the file paths are identical on the new server, you won't need to do anything. The Web File Share installation will just work with everything in its place.

If the user files paths no longer match on the new server, you will be required to update them in the MySQL database. The following SQL queries can be ran, via either a tool such phpMyAdmin, or directly from the MySQL command line client:

```
UPDATE `df_modules_search_index_queue` SET `path` = REPLACE(path, '/YOUR/OLD-PATH/', '/YOUR/NEW-PATH/');
UPDATE `df_modules_search_index_queue` SET `path` = '/YOUR/NEW-PATH' WHERE `path` = '/YOUR/OLD-PATH';

UPDATE `df_paths` SET `path` = REPLACE(path, '/YOUR/OLD-PATH/', '/YOUR/NEW-PATH/');
UPDATE `df_paths` SET `path` = '/YOUR/NEW-PATH', `filename` = 'NEW-PATH' WHERE `path` = '/YOUR/OLD-PATH';

UPDATE `df_users_permissions` SET `homefolder` = REPLACE(homefolder, '/YOUR/OLD-PATH/', '/YOUR/NEW-PATH/');
UPDATE `df_users_permissions` SET `homefolder` = '/YOUR/NEW-PATH' WHERE `homefolder` = '/YOUR/OLD-PATH';

UPDATE `df_modules_user_roles` SET `homefolder` = REPLACE(homefolder, '/YOUR/OLD-PATH/', '/YOUR/NEW-PATH/');
UPDATE `df_modules_user_roles` SET `homefolder` = '/YOUR/NEW-PATH' WHERE `homefolder` = '/YOUR/OLD-PATH';
```

You will need to replace /YOUR/OLD-PATH, /YOUR/NEW-PATH and NEW-PATH above with your actual server file paths. You will need to respect the trailing slashes. You will be replacing /some/old/path with /some/new/path and /some/old/path/ with /some/new/path/.

Make sure you always use forward slashes (/), even on Windows servers (example: c:/your/path).

Make sure the case are used as before. If a user's home folder was previously set to /my/User, do not change to /my/user even if your new file system might be case insensitive.

Installing updates

To install software updates please follow these steps:

1. Access your Web File Share installation and log in as superuser (The default login name of the superuser is “admin”).
2. Open “Control Panel”
3. Go to “System configuration” » “Software update”
4. (Important!) In most cases, the software updates install easily with just a click from the Web File Share control panel section. However, if your Web File Share installation is under production and people depend on its functionality, we strongly recommend you to make a full backup of it before installing the update. If the update's installation fails, you will need to restore this backup to get Web File Share back online.
5. If PHP will not be able to replace a file, because of its permission settings, the update will fail and the Web File Share installation may become unusable. To avoid this, please try to set the permissions of the the entire Web File Share installation folder so that PHP can replace all files without problems. You will be able to set the permissions back, after installing the update. Also: make sure the MySQL user that Web File Share is configured with, has temporary ALTER and DROP permissions. You can remove this permission after you are done with the updates.
6. Click “Check for updates” and wait while Web File Share shows the result.
7. Read carefully the update's description and notes.
8. Click “Download update” and wait for the update to download.
9. Click “Install update” to install the update.
10. Read the update log carefully and check for error messages. If you encounter errors that you do not know how to fix, drop us a quick message.

If you are having troubles with file permissions on Linux servers, please contact your server administrator to help you make sure PHP has write access over the Web File Share application files.

If you are using Microsft IIS web server, you need to right click the Web File Share installation folder and add the system user “IUSR_<computer-name>” (Internet guest account) user to the list of users who have access to the folder, enabling the “Modify” and “Write” permissions.

Recovering a broken installation

If you ignored the advice about creating a backup, tried to install an update and failed, leaving your Web File Share installation unusable, here are the steps to fix it:

(You can still make a backup of the broken Web File Share installation folder and its database now, to avoid loosing your user accounts, settings and documents by mistake!)

1. You need a Web File Share installation kit that matches the Web File Share version you were last running, before it got broken. It is important that you have the exact same version, because you are going to replace the application files and these need to match the MySQL database structure.
2. Move the folder “system/data” (and any other file that you might have customized and the update did not overwrite) from the broken installation to a safe location.
3. Delete the Web File Share installation folder (after making sure you have the folder “system/data” in a safe location)
4. Extract the contents of the Web File Share installation kit mentioned at step #1, at the exact same location of your old installation. It is very important to have the application files in the same location as before and not in some other folder.
5. Replace the newly extracted “system/data” folder with the old one, the one you saved to a safe location at step #2
6. Access your Web File Share installation using the browser and make sure things work as they used to, before installing the update.
7. Make a backup of your now working Web File Share installation and follow the above update installation guide, without skipping any step ;)

Upgrading PHP to version 7

The Web File Share application files that are currently in use on your PHP 5 server were designed to be used specifically with that version of PHP. Upgrading to version 7 will make the Web File Share installation stop working. The solution is to replace the application files with a new set, from a PHP 7 Web File Share installation package. This can be done before or after upgrading the PHP version. It makes no difference, as the Web File Share installation would not be accessible either way. The Web File Share version of the installation package which you'll be using needs to match the exact Web File Share version which you are currently running.

To determine which Web File Share version you are currently running, sign in as superuser, open the control panel and navigate to “Software update”.

If, for example, you are running version 2016.11.07 you will need the installation package named Web File Share_2016_11_07_PHP7.zip. Note the “PHP7” part in the filename. The latest Web File Share version can always be downloaded from our homepage, but if you wish to upgrade an older Web File Share version, contact us for receiving an appropriate installation package for your version.

Let's assume you are updating version 2016.11.07 and your Web File Share installation folder is located inside /www/WebFileShare/. Please follow these steps:

1. Make a backup of your folder /www/WebFileShare/. Preferably on a completely different server/computer.
2. Create a subfolder /www/WebFileShare/@old.
3. Move everything from /www/WebFileShare/ to the @old subfolder.
4. Extract the archive WebFileShare_2016_11_07_PHP7.zip inside /www/WebFileShare
5. Delete (or rename/move - just to be safe and make sure you are not deleting the wrong folder) the folder /www/WebFileShare/system/data.
6. Move the folder /www/WebFileShare/@old/system/data inside /www/WebFileShare/system/. (This basically transfers over your settings and data.)
7. If you are getting a licensing error, simply access http://YOUR-SITE.COM/WebFileShare/?alicense=1&key=YOUR-WebFileShare-LICENSE-KEY to update the license.
8. After confirming that the installation is working fine, you can delete the remaining /www/WebFileShare/@old subfolder.

And that's it. If you have upgraded PHP to version 7, then the WebFileShare installation should also be up and running now.

Changing the MySQL connection information

You can change the MySQL connection information inside the file “system/data/autoconfig.php”.

Simply open the file in a text or code editor and make the appropriate changes.

Deleting old files

The following command line script can be used for deleting old files from users home folders.

```
php cron/delete_old_files.php  2592000 admin confirm
```

2592000 is 30 days in seconds, admin is the username of the account that is being cleaned and confirm is needed for executing the task. If confirm is omitted then the command will only simulate the action, showing you what will happen without actually deleting the files. If the username is omitted, the process will run for all user accounts in the system. 2592000 is the smallest value you can use, preventing you from deleting files younger than 30 days.

Important note: the date used for determining a file's age is the “modified” date, not the “created” date. If you have files created a long time ago, but were recently modified, they will not be deleted. For any other desired behavior, the file “system/modules/fileman/sections/cli/php/delete_old_files.php” is freely editable.

Upgrading to PHP 5.5 or 5.6

If you were running a recent Web File Share version on PHP 5.3 or PHP 5.4, you should be able to update PHP to 5.5 or 5.6 without any change made to the Web File Share installation.

Overview

Roles can be used to easily apply sets of permissions to multiple users at the same time.

If you select a role for a user, you will no longer be able to set individual permissions and settings for that user.

Deleting a role

To delete a role follow these steps:

1. Open the control panel.
2. Select “Roles”.
3. Select the role you want to remove.
4. Click “Delete role”.
5. Click “Delete” to confirm the role's deletion.

Deleting a role will not delete any user account.

Deleting a role will not delete any user account.

Adding a role

To create a new role follow these steps:

1. Open the control panel.
2. Select “Roles”.
3. Click “Create new”.
4. Fill in they form:
5. Required fields:
   - Role name
6. Click “Submit” to create the role with the specified details.

Editing a role

To edit a role follow these steps:

1. Open the control panel.
2. Select “Roles”.
3. Select the role you want to edit.
4. Click “Edit role”
5. Make the appropriate changes in the form.
6. Click “Submit” to save the changes.

Choosing A Hosting Service

WebFileShare works with most hosting service, with either their shared or dedicated plans. If you are using a dedicated, VPS, or any other type of virtual dedicated server, it is guaranteed that WebFileShare will work great for you.

The following is a note for people using shared/budget hosting plans, the ones that usually charge less than $5/month. These cheap plans are very good for hosting a simple website. However, some of them are not suitable for running a serious application like WebFileShare. That is because most WebFileShare processes require:

1. a larger amount of server RAM memory
2. longer PHP script execution times
3. longer client requests (large uploads) and longer server replies (large downloads)

These are expensive resources and the hosting companies limit clients access to them, to be able to host a large number of clients on a small number of servers, and keep the costs low. These servers are configured to automatically stop requests that are taking a long time to execute. So if you have users with low bandwidth (poor Internet connections), that require a very long time to upload or download even the smaller files, you should look for a better hosting plan, like a VPS, where you are allowed to use more server resources and for longer periods of time.

If you are mostly dealing with documents, small image files or other types of files with sizes that do not exceed 100MB, a budget hosting service can work quite fine.

We recommend that before purchasing a WebFileShare license, contact us to help you review the server configuration, to make sure WebFileShare will work great for you.

Installing ionCube on Top Hosting Providers

Installing ionCube on Ubuntu

Please see https://www.digitalocean.com/community/tutorials/how-to-install-ioncube-on-ubuntu-16-04

Shared Hosting Support

On the PHP details page, search for the “ioncube” word. If you can't find anything similar, then it is not enabled. Search the hosting FAQ, forum for any instruction to enable ionCube. The best solution would be to contact your hosting support. It is just matter of seconds for them to enable ionCube for you.

Installing ionCube on 1&1

For Linux packages, please follow this link: http://help.1and1.com/hosting-c37630/scripts-and-programming-languages-c85099/php-c37728/manually-install-ioncube-loader-a726806.html

Installing ionCube on HostGator

1. Log into the HostGator cPanel – yourdomain.com/cpanel
2. Go to the Software » Services in cPanel
3. Click the “PHP Config” option and select the “PHP5 (Single php.ini) option
4. And click “Save Changes.”

You will be directed to Install Default php.ini page

1. Click the option to install IonCube.
2. Check “IonCube” and click “Install” button to install.
3. Use te “Go Back” option from bottom once done
4. Go to your “File Manager”
5. Select Web Root (public_html/www) to load in file manager
6. Browse and find newly created php.ini.default
7. Select and Rename the file as php.ini
8. Now the IonCube is enabled.

Installing ionCube on Just Host

https://my.justhost.com/cgi/help/149

Installing ionCube on iPage

http://members.ipage.com/knowledgebase/beta/article.bml?ArticleID=950&type=How%20To#Nugget_1034

Installing ionCube on Blue Host

https://my.bluehost.com/cgi/help/149

Installing ionCube on Hostmonster

https://my.hostmonster.com/cgi/help/149

Installing ionCube on Fatcow

Contact hosting support

Installing ionCube on Blue Domino

- Log into the Control Panel with the account username and password.
- Click on CGI and Scripted Language Support under Scripting and Add-Ons.
- Click on PHP Scripting.
- Add the following line:

zend_extension = /usr/local/lib/ioncube/ioncube_loader_lin_x.x.so

(Where x.x is the version of your php)

- Click on the Save button

Installing ionCube on Dreamhost

http://wiki.dreamhost.com/IonCube_Loader

Installing ionCube on Glow Host

Must open a support ticket and request Ioncube support.

Installing ionCube on Godaddy

http://support.godaddy.com/help/article/5608/installing-ioncube-on-your-linux-hosting-account

Installing ionCube on IPOWER

http://www.ipower.com/knowledgebase/read_article.bml?kbid=6041

Installing ionCube on Jaguar PC

http://www.jaguarpc.com/support/kbase/index.php?action=list&faq=697

Installing ionCube on Lunarpages

https://support.lunarpages.com/knowledge_bases/article/317

Installing ionCube on OVH

Add the following line to a custom .htaccess file:

```
SetEnv IONCUBE 1
SetEnv PHP_VER 5
```

Or create a file called .htaccess, and using a text editor put the above code lines in it, save changes, and upload it to the root of the store files.

Installing ionCube on Pow Web

http://www.powweb.com/knowledgebase/read_article.bml?kbid=6041

Installing ionCube on Netfirms

http://support.netfirms.com/idx.php/0/831/article/How-do-I-use-Ioncube-with-my-site.html

Installing ionCube on Site Ground

http://kb.siteground.com/article/Is_IonCube_supported.html

Installing ionCube on Start Logic

http://www.startlogic.com/knowledgebase/read_article.bml?kbid=6041

Installing Ioncube Loaders

Assisted installation (Loader Wizard)

The “Loader Wizard” is a PHP script that can help you with the installation. Download the script file from the ionCube website and upload it to your server. Launch the script in your browser for guidance on installation and selection of the correct Loader package. For more info you can refer to http://www.ioncube.com/loader_installation.php

Checking if ionCube is installed

Type http://yourdomain.com/webfileshare/info.php

If “info.php” does not exist, create one and add the following code inside:

```
<?php
phpinfo();
```

Now “http://yourdomain.com/filerun/info.php” should provide information about your PHP configuration, as in the following example:

Choosing the right version

The first highlighted item describes the PHP version and server OS details e.g. PHP 5.5 in Ubuntu 3

Second item describes the system processor type e.g. x86-64. This is needed to download appropriate loaders e.g. as in image Linux (x86-64) package. You should enable the correct loader file with OS type and PHP version e.g.

```
zend_extension = /usr/local/ioncube/ioncube_loader_lin_5.5.so
```

The third highlighted item tells if PHP is threaded or not. In this example PHP is not threaded, if thread safety is enabled then your PHP configuration line should look like this:

```
zend_extension = /usr/local/ioncube/ioncube_loader_lin_5.5_ts.so
```

(note the “_ts” part)

Manual "ionCube" installation

You can do it your self, if you have access to the PHP configuration file “php.ini”. Most hosting service allow you to either create a custom PHP configuration file inside any of your folders, or they provide a PHP configuration editor inside their control panels.

Depending on the PHP details that you checked above, your configuration line might look like this:

For linux and php 5.5, add a line like this:

```
zend_extension = /usr/local/ioncube/ioncube_loader_lin_5.5.so
```

For FreeBSD and php 5.3, add a line like this

```
zend_extension_ts = /usr/local/ioncube/ioncube_loader_fre_5.5_ts.so
```

For Windows and php 5.5, add a line like this

```
zend_extension_ts = c:WINNTioncube_loader_win_5.5.dll
```

It is always best and easier to contact your hosting company tech support and ask them about the appropriate configuration line.

Shared Hosting Support

On the PHP details page, search for the "ioncube" word. If you can't find anything similar, then it is not enabled. Search the hosting FAQ, forum for any instruction to enable ionCube. The best solution would be to contact your hosting support. It is just matter of seconds for them to enable ionCube for you.

Loader Wizard

The "Loader Wizard" is a PHP script that can help you with the installation. Download the script file from the ionCube website and upload it to your server. Lunch the script in your browser for guidance on installation and selection of the correct Loader package. For more info you can refer to http://www.ioncube.com/loader_installation.php

Activity notifications

Since version 301013, Quik File Share provides a way for the users to quickly see changes made by other users.

On the right side of the folders menu, there is a new option that opens a drop-down menu showing a log with the latest actions performed by other users anywhere inside your home folder.

The icon of the option is black and white when there are no notifications and blue when there are. There is also an overlay that shows the number of new actions.

Unless the real-time notifications are enabled, as described below, the notifications will be updated every time the user accesses a new folder or clicks the "Refresh" button to reload the list of files.

To see what actions have been performed by other Web File Share users inside your home folder, access the “Folder Activity” tab available on the “Details and activity” panel on the right side of the user interface. To see the tab, access the folder without selecting any items inside.

Real-time notifications with Pusher.com

The notifications can be made real-time, by enabling Pusher.com integration:

1. Signup for a free Pusher API account at http://pusher.com/pricing
2. Access the Web File Share control panel as superuser and go to “System configuration” > “Misc options” section.
3. Enable the main checkbox and configure the App ID, Key and Secret that you get from your Pusher.com account.

The users will be notified in real-time about files that have been uploaded, files that have been downloaded, previewed or commented by other users.

Disabling the sound

Each user can enable/disable the sound notifications from their Account Settings panel. The preference persists between browser sessions, so the user will not have to use the toggle every time he is accessing Web File Share. The sound is enabled by default for all users. To mute it by default, add the following to the configuration file:

```
$config[['app']][['disable_sound_notification']] = true;
```

The sound played on notification can be customized by replacing the two files “sounds/new.mp3” and “sounds/new.ogg”.

Limitations

- The users will be notified only about actions performed inside their own home folder. They will not be notified about actions performed in folders that are shared to them by other users.
- If user doesn't have permission to read file comments in its own home folder, the number of new events will still increase when comments are being added.
- This feature doesn't work properly with hidden folders. Users will be notified about actions performed inside hidden folders, so you will wish to disable the feature for the users with hidden folders. (The option for hiding folders will be dropped in future versions)

Disabling the feature

This feature is connected to the “file-based activity logs” feature. Disabling the user's “User can access the files' activity logs” permission, will disable this feature as well.

File-based Activity Logs

Web File Share keeps an activity log for each file available in the users' home folders. This is completely independent of the user activity log that is accessible by the admin users in the control panel. This log allows the users to see a history of everything that happened to the file trough Web File Share.

Note: making changes or accessing files using third-party methods will not be visible in these logs.

It can be globally disabled from “Control Panel » System configuration » Misc options”. While disabled, no activity will get logged on the files, although existing records will not get deleted and will be accessible once the feature is enabled again.

It can also be enable/disabled per user or role, from the list of user permissions.

Activity logs can be accessed only on files located inside the user's home folder. The activity logs of shared files are not accessible. Not even inside anonymously shared folders. So users can share folders without worries that the history of their own actions will be shown to other users.

Additional details are displayed for certain actions. For example, sending a file by e-mail will show the list of recipients. However, only the user that performed the action and the admin users are able to see these details.

Mozilla Thunderbird FileLink Addon

This is an add-on to be used with Mozilla Thunderbird e-mail program.

This add-on allows you to easily e-mail large file attachments by uploading those attachments to your Web File Share user account and then inserting a web link to the file into the body of your email.

The add-on will not require you to share your Web File Share username and password with Thunderbird, but instead it leverages Web File Share's OAuth2 server to authorize Thunderbird to perform limited operations on behalf of your Web File Share account.

Files uploaded to Web File Share through this add-on will be located inside the automatically created folder “Apps/Thunderbird”.

Note: Thunderbird will not have access to any other folder and will not be able to perform other operations with your Web File Share user account.

Alternate downloads

If your RAW photographs are very large and it takes a long time for WebFileShare/ImageMagick to generate a preview, or your 4K videos cannot be previewed by clients with slower Internet connections, it can be more practical to share with your clients a folder containing low resolution versions of your media. To still provide the users with the option of downloading the high res/raw version of the files, you can use this plugin. It will add an “Open with..” option called “Alternate Download”. To enable the plugin, edit it from the “Files” → “Plugins” control panel section and set a configuration JSON.

You can configure as many folders with alternate downloads as you wish. Here's an example configuration:

```
{
 "paths": [{
  "normal": "/your/files",
  "alternate": "/your/alternate/files",
  "extension": "jpg"
 }]
}
```

- 'normal' is the folder you wish to enable the plugin for.
- 'alternate' is the path of the folder you wish to use for the source of alternate files.
- 'extension' is optional, if the alternate files have a different extension than the one selected by the user.

Note that the download actions are being logged to the normal file (the file which was selected by the user), not to the alternate file. You can see when a user is downloading the alternate version of the file when the download log entry shows “alternate_download” in the details.

P.S. The folders containing alternate versions need not be accessible by the Web File Share user.

Metadata

Metadata is information that a file can have attached to it. You can attach information like: comments, title, author, tags, etc.

Fields

Metadata information is stored in metadata fields. You manage the fields from inside the “Control Panel » System configuration » Metadata” administrative section.

When setting up a metadata field, you can define a list of options. The user will be presented with the predefined list to choose from. If you do not define a list of values, the user will be free to type in any value he wishes.

Field sets

Every metadata field needs to be part of a metadata field set. Field sets can be used to group more fields.

File types

To automatically associate certain field sets with certain types of files, you define metadata file types. You might want, for example to have a set with fields such as “Photographer”, “Camera”, “Location” associated with image files, so that when you edit the metadata for an image file you are presented by default with these fields.

By defining a field set as generic, its fields will be automatically displayed inside the metadata window, no matter what “file type” the user selects for the file.

Metadata information can be displayed in the list of files as new columns, by clicking the arrow icon that appears while holding the cursor over a column's header and selecting the metadata fields from the list of possible columns.

Metadata fields, filed sets and file types created by independent admin user are available only to these users and the user accounts he creates.

Desktop sync

You can keep your remote folders in sync with your local ones, or the other way around with the desktop sync apps.

On the first run, you will be asked to provide your Web File Share installation URL, your Web File Share username and password. You can either sync your entire account, or choose particular folders.

Mobile apps

To be able to use the mobile apps with your Web File Share installation you need to enable the API.

A SSL enabled web server is required. (Your Web File Share URL needs to start with “https://” and not “http://”).
(For testing only, you can temporarily enable the API via “http://”. See “Testing without SSL”)

Please follow these steps:

1. Login to the Web File Share installation as superuser.
2. Open the control panel.
3. Select “API” from the menu (under “Security”).
4. Select the “Enable API” checkbox.
5. Click “Save Changes”.

Upload problems

Drag & drop upload mode

The "Drag files from your computer here" text is not displayed

The drag&drop upload mode requires Java support enabled in your browser. You can clickhere to verify if it's enabled and up to date.

The progress bar stays at 0%

Please make sure you have confirmed the Java security prompt, as described in the following image. If you have already clicked "Cancel" you will need to close the browser and reopen it, in order to see the security prompt again.

The file is not on the server after the transfer is completed

There are multiple possible causes for this:

Your computer uses a proxy server: The Java upload applet cannot inherit the browser's proxy settings so you will need to add these settings into Web File Share by clicking the "Proxy settings" link available under the drag&drop area.

File permissions: The folder where you want to upload doesn't have write permissions.

Error: *Please specify a file for upload.*

Most probably the "Drag&Drop upload chunk size" you have configured inside the "Control Panel » System configuration » Misc options" administrative section is higher than your "upload_max_filesize" or "post_max_size" PHP configuration directives. Please note that a larger chunk size will not help you upload larger files, on the contrary, it will prevent the drag&drop upload mode from avoiding the limitations of your server. If you are getting this error please set the value back to its default value (2MB).

A login prompt keeps popping up

Please make sure "session.use_only_cookies" is set to "Off" in your PHP configuration.

Error: *Upload failed: javax.net.ssl.SSLHandshakeException: [...] unable to find valid certification path to requested target*

You are using a self-signed SSL certificate or the certificate that you are using was not installed properly on your web server.

Please try following these steps:

1. Locate your intermediate bundle file and open it. When you open it, you will see 2 different areas starting with BEGIN CERTIFICATE.
2. Cut the top certificate starting at "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----".
3. Paste it below the next certificate so it is now at the bottom of the file. Save file and restart the web server.

If this information doesn't look familiar to you, please contact your server administrator or hosting service tech support to help you with this issue, as it is not Web File Share related.

Error: *Failed to upload file. creation failed: copyFile error: source file /tmp/php7B.tmp doesn't exist*

PHP doesn't have permission to place files in the temporary folder. You need to give write permission over the "upload_tmp_dir" configured PHP folder to the user under which PHP is running. If "upload_tmp_dir" is not specified, PHP will use the system's default temporary folder.

Login problems

Error: *The path of your home folder doesn't point to an existing folder.*

When setting a user's home folder path, please use the "[Check path]" button next to the text input, to make sure the path is valid and points to an existing folder.

If the account is using a role, you need to check the role's settings to see if the path is correct.

If you are receiving this error when logging in as superuser, you can fix it by accessing the control panel directly, by the following URL: http://*www.your-site.com/WebFileShare*/panel/

The HTTP authentication for the mobile version doesn't work

If PHP is installed as CGI, please try to create a file named ".htaccess" inside the root folder of your Web File Share installation and write the following inside:

```
RewriteEngine on

RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L]
```

Apache module "mod_rewrite" is required for this to work.

Downloading problems

Internet Explorer over HTTPS: Internet Explorer Cannot Download [...]

Please set "session.cache_limiter" to "private_no_expire", in your PHP configuration. It should fix the problem. The problem is caused by a weird Internet Explorer behavior.

Downloading very large files

For FastCGI Servers (Usually Microsoft IIS)

If the transfer stops for no apparent reason while downloading large files, try increasing the values of "RequestTimeout" and "ActivityTimeout" FastCGI configuration directives (on Windows servers, the location of the file is usually "%WINDIR%system32inetsrvfcgiext.ini"). The default values do not accommodate downloading large files over slow Internet connections.

For Apache Web Servers

Applies to Web File Share version (020710A)

Most shared hosting services configure the servers so that PHP scripts that are running for too long (usually more than 30 seconds) and use to much CPU or memory are automatically stopped. This is to save money by crowding as many customers as possible on a single server. Downloading large files trough PHP, using a slower internet connection can take quite a long time, requiring the PHP process to run for a few minutes. If your large downloads do not complete successfully, you might want to take advantage of this workaround. This will make Web File Share pass the download to the web server (Apache), instead of letting PHP deal with it.

Requirements

1. Apache web server (it doesn't work with IIS or other web servers)
2. Apache module "mod_rewrite" needs to be enabled
3. (on Linux servers in particular) the users under which Apache is running (usually "www" or "apache") must have permission to access the files that are to be downloaded. Sometimes Apache's access is limited to the "www" or "public_html" folder and additional permissions must be configured.

To enable the workaround, please follow these steps:

1. Open "/path-to-WebFileShare/customizables/config.php" in a text editor
2. Copy the following three lines of PHP code at the end of the file:

```
$config['enable_download_trick'] = true;

$config['download_trick_minimum_filesize'] = 20971520;//in bytes, recommened value: 20971520 (20MB)

$config['download_trick_links_life'] = 10; //in seconds, recommended value 10
```

1. If the code already exists in the file, you can simply replace "false" with "true".
2. Make sure a file named ".htaccess" is availabe inside the folder "/path-to-WebFileShare/download". If a file "htaccess.txt" exists in the folder, please rename it to ".htaccess".

Troubleshooting

If you are getting a "500 Internal Server Error" when trying to download files, most probably "mod_rewrite" is not available on your server.

If you are getting a "404 File Not Found" error, please make sure the file ".htaccess" is located in the folder "/path-to-WebFileShare/download", it is not empty and has proper permission settings. If you are accessing the Web File Share installation using a subdomain, you should add "RewriteBase /download/", right after "RewriteEngine On", inside the ".htaccess" file.

Large files (>2GB)

Linux: Files larger than 2GB do not show up in the list.

On Linux servers, PHP needs to be configured with LFS (Large File Support) in order to be able to manage files larger than 2GB. Please read here more about it: http://www.php.net/manual/en/intro.filesystem.php

Zipping files and folders

Creating zip files from larger files, or folders containing many files, it might take a longer time than allowed by the default PHP configuration. You can allow WebFileShare/PHP more time, to be able to complete the task. This can be done by increasing the value of the "max_execution_time" PHP configuration directive, which has a default value of "60" (seconds).

Metadata

Metadata is information that a file can have attached to it. You can attach information like: comments, title, author, tags, etc.

By default Quick File Share provides ways of attaching comments to files using the "Comment" contextual menu option. For any other type of metadata you need to use the "Metadata" contextual menu option.

Metadata information is stored in "metadata fields". You manage the fields from inside the "Control Panel » System configuration » Metadata" administrative section.

When setting up a metadata field, you can define a list of options. The user will be presented with the predefined list to choose from. If you do not define a list of values, the user will be free to type in any value he wishes.

Every metadata field needs to be part of a "metadata fieldset". Fieldsets can be used to group more fields.

To display certain fieldsets for certain files, you define "metadata filetypes". You can choose for each filetype what fieldsets to be displayed. By defining a fieldset as "generic", its fields will be automatically displayed inside the metadata window, no matter what "file type" the user selects for the file.

Metadata information can be displayed in the list of files as new columns, by clicking the arrow icon that appears while holding the cursor over a column's header and selecting the metadata fields from the list of possible columns.

Metadata fields, filedsets and filetypes created by independent admin user are available only to these users and the user accounts he creates.

To add fields to the field set

1) Open the Field set in the "Edit" mode.

2) Click "Add" button under the "Fields" section.

3) Define the field and click "Add Field" button.

4) When you click on "Field sets" again, you'll see that the number under "Fields" column has been incremented. This indicates that a new field has been successfully added to the Field set.

How to define Metadata Filetypes

To display certain field sets according to the file types like PDF, PNG, docx etc., you can define "Metadata Filetypes"

1) Select "File Types" under Metadata from the control panel.

2) Define the "File type" by giving an appropriate name and selecting the field set that should display for that particular file type. Click on "Add File Type" button to save file type.

Configuring users’ file access

Basics

Each user has a home folder, which is an actual folder on the server's file system. Users do not have more than one home folder. This folder is assigned using the “Home folder” field available under the “Permissions” tab, when adding or editing the user accounts. It must be a path to an existing file system folder.

The user is able to browse all the subfolders available in his home folder.

Two users with the exact same “home folder” path will access the same files. To prevent the users from seeing each other's files, make sure the users have different “home folder” paths.

Important: make sure the users home folders are located outside the public area of your web server. In other words, files that users upload to their home folders should not be accessible directly by accessing your website's address like this: http://www.your-site.com/webfileshare/users-folder/private-file.txt So, make sure the home folder paths do not contain any of the words “public_html”, “html”, “www” or “*your-domain.com*”.

Providing admin user with access to all users files

The most common setup keeps the users access separate while allowing the admin users or superuser to access everything. To achieve that, make sure you create the users home folders inside the same root folder and assign the root folder as home folder for the admin users. Here's an example:

User A's home folder: `/storage/files/users/user_a/`

User B's home folder: `/storage/files/users/user_b/`

Admin's home folder: `/storage/files/users/` *(The admin can access all the users files)*

Superuser's home folder: `/storage/files/` *(The superuser can access even folders one level higher - to store files which other admin users cannot access)*

Accessing more than one folder

To allow the user to access files located outside his home folder, you need to use the folder sharing system. Logged in with a user account which has access to another location (usually an admin account), right-click the desired folder and select "Share.." -> "with users".

The shared folders will appear for the users under their home folder, like in the following screenshot. In this example, there is a folder shared by "Isha" and one shared by "John":

To make the shared folders appear on the same level as "My Files", check the option "Share anonymously", available under the "Options" tab when sharing: