Web File Manager

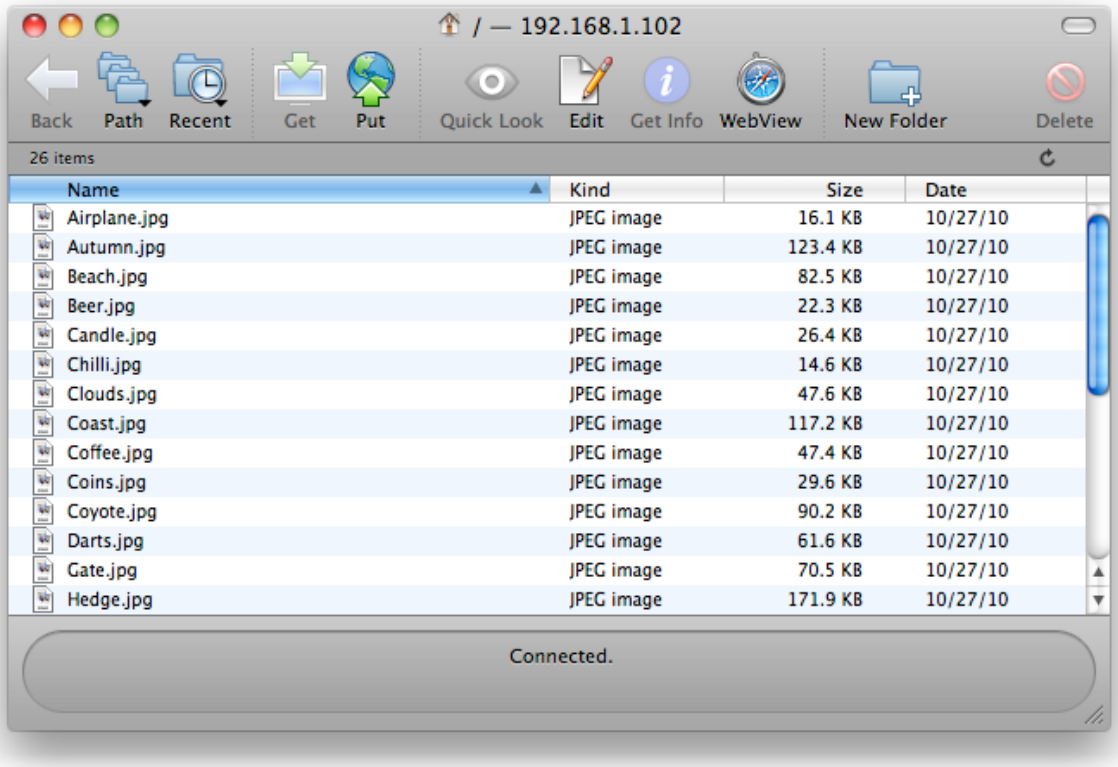
Contents

Overview

Popular Web browsers have long included basic support for FTP. But because FTP is a secondary task for Web browsers, these clients usually include extremely basic and often bug-ridden FTP implementations. So, when users need to access your server using a Web browser, we very strongly recommend that they use the Rumpus Web File Manager, which provides not only a more attractive and easier to use interface, but a more reliable and consistent one as well.

True FTP does offer some advantages over the WFM. For example, most FTP clients support uploading entire folders of content at one time, which is something Web browsers simply don't support. When a user needs to routinely transfer large numbers of files to your server, they may be better served by a dedicated FTP client like Fetch, Transmit, or CuteFTP. However, for less technical users that don't normally transfer large numbers of files, the Rumpus WFM is usually the best option.

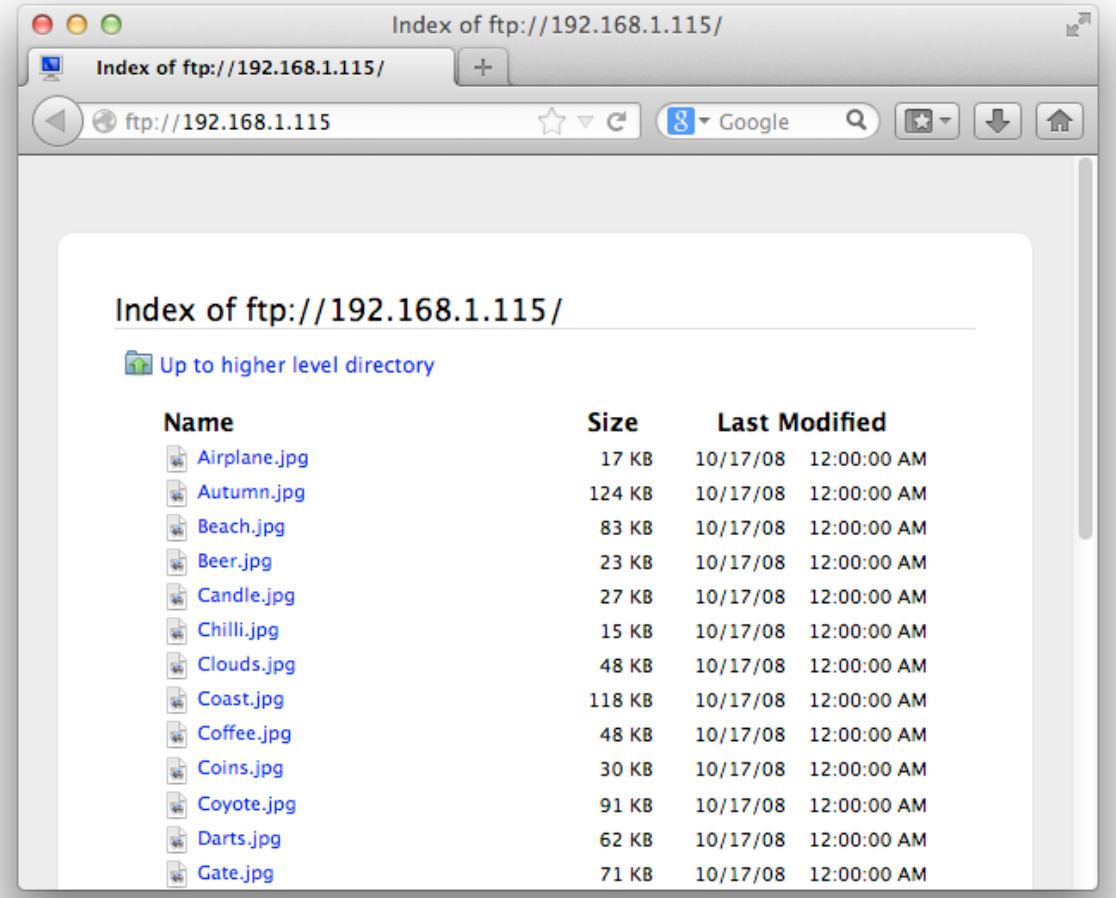
Here is a sample Rumpus server, accessed via Fetch, a popular FTP client for the Mac.



Accessing a Rumpus server via FTP using Fetch

Again, Fetch and other dedicated FTP clients work great with Rumpus, and are recommended for technically savvy users with extensive file management needs.

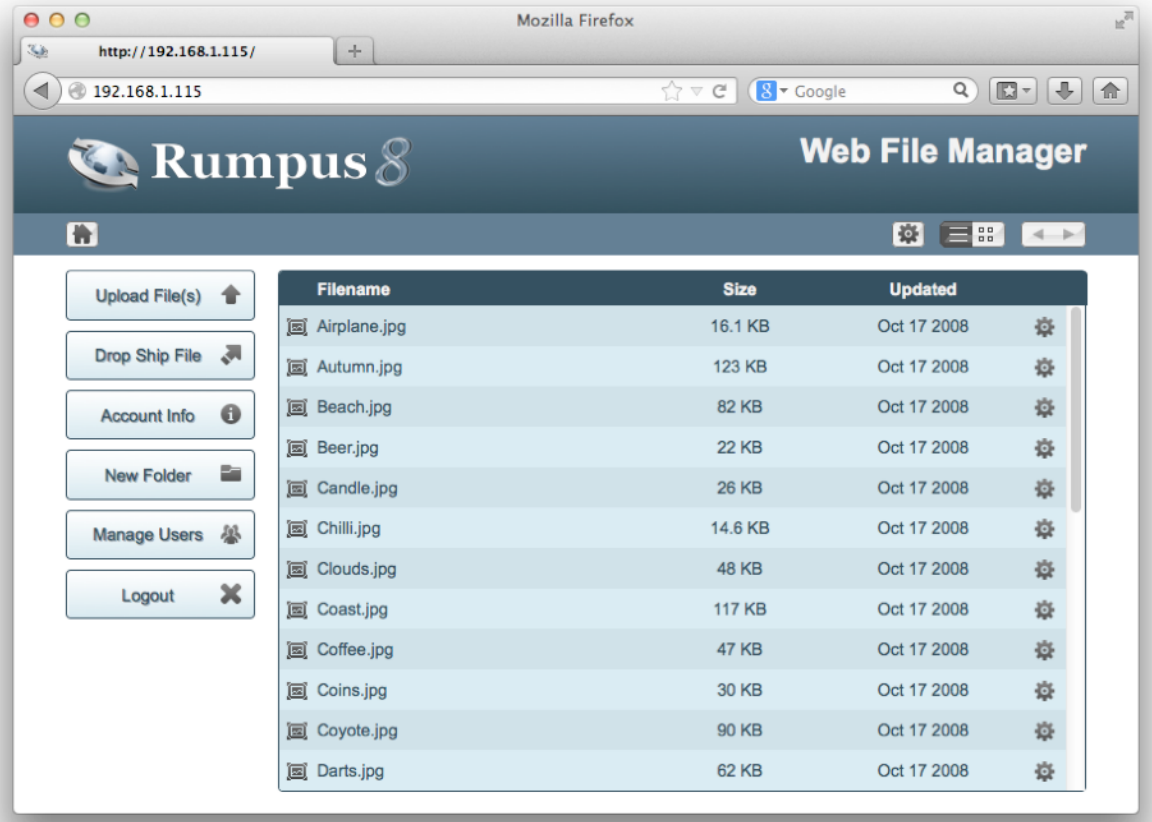
If, however, a user tries to use a Web browser to access the server, problems may arise. Not all browsers support FTP (such as Safari, for example), and others won't automatically prompt for the username and password, instead requiring that this information be included as part of the URL. When a user does log in using a popular Web browser, they will see something like this:



Display of an FTP file listing in a typical Web browser

The interface isn't bad, but it isn't customizable, and doesn't make it clear how to upload files, download files, create folders, etc.

Now, here is the same browser, accessing the same server via the Web File Manager:



Display of the same listing through the Rumpus Web File Manager

The WFM interface is easier to use, more professional looking, and easy to customize to be displayed with your company colors and logo. Also, users can easily connect using any Web browser simply by entering the IP address or domain name of your server.

The WFM respects all of the same user settings and server preferences you have defined for FTP, too. This means that you configure your server once, and users have the choice of using traditional FTP or the Web File Manager. In fact, the same user can use FTP for one session and the WFM for the next, if they like. From a server administration standpoint, there is no difference.

Getting Started

The WFM respects all of the user account setup and other security configuration from your FTP site and is enabled automatically when Rumpus is installed.

The most basic server settings, including fundamental Web service options, can be found on the Settings window, Settings tab. Note that the standard HTTP port is 80, but Rumpus may, depending on whether or not another Web service is already running, default to 8000 to avoid a conflict. If no other Web server is running, set the port to 80, otherwise, use port 8000 or choose some other suitable port number.

To connect to the server, use a standard HTTP URL in any Web browser, specifying the IP address (or domain name) of the server and the port (if the Rumpus Web server is configured for a port other than the standard port 80). For example:

```
http://192.168.1.1:8000/
```

In this example, replace "192.168.1.1" with the IP Address or domain name of your server, and replace "8000" with the port number specified in Rumpus. If you set the Rumpus port number to 80, you don't need to specify the port at all, so use the URL:

```
http://192.168.1.1/
```

The local access URL is shown in the "Get Connected" window in the Rumpus control application.

If you have trouble connecting to the WFM interface, make sure that there is no firewall enabled on the server. If a firewall is in use on the server, disable it, at least temporarily, to confirm that you can access the Rumpus service. Once you have confirmed connectivity to the server, you can re-enable the firewall and configure it to allow access on the necessary ports.

When using Rumpus' default WFM settings, you will next be presented with the user login page. Enter a valid Rumpus user account name and password to complete the login.

Web Browser Compatibility

The Rumpus Web interface has been designed to take advantage of the latest capabilities in Web browsers, while optimizing the interface to the best of older client's technologies. The best WFM interface possible is displayed to modern browsers, including:

Safari 7 and later

FireFox 16 and later

Google Chrome 26 and later

Microsoft Internet Explorer 10 and later

For the best possible user experience, we recommend that clients use one of these browsers, all of which are widely available for download.

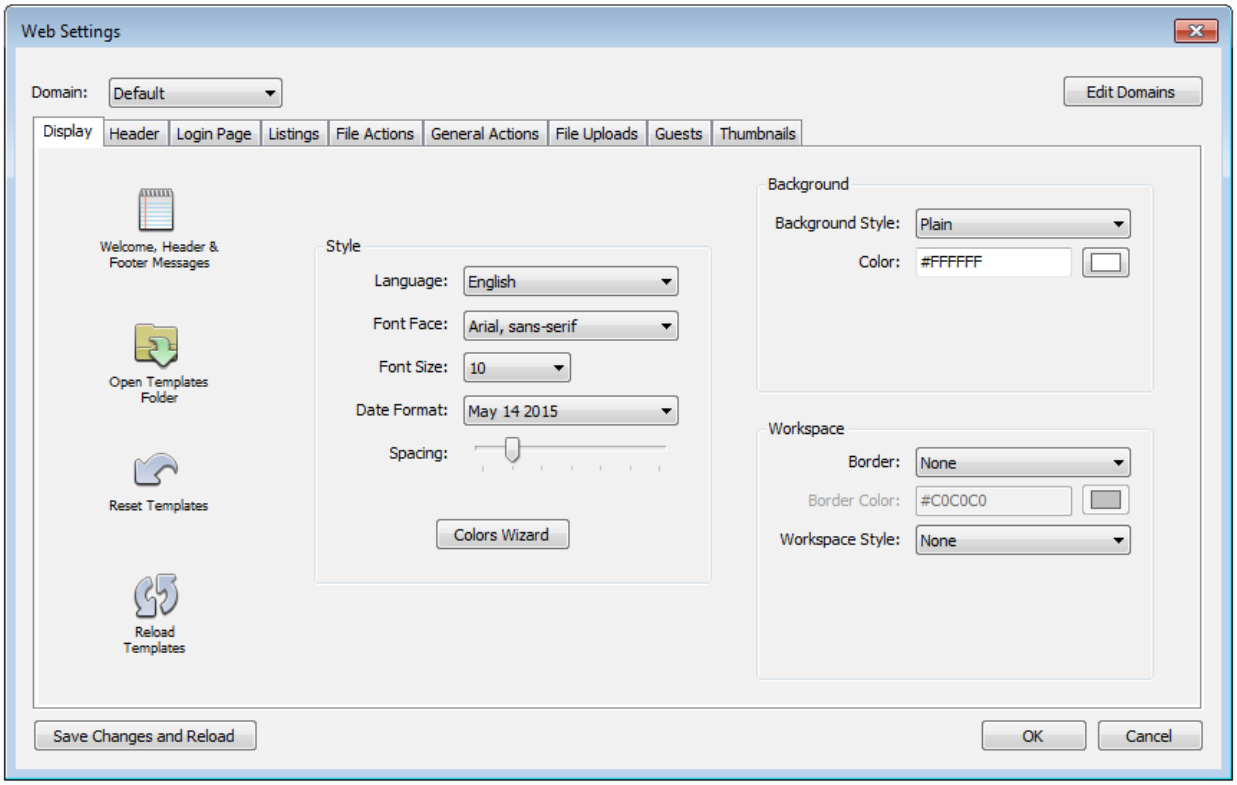
Older Web browsers, however, are also supported. Users of Safari 5 and 6, for example, will be presented with an interface that is nearly indistinguishable from Safari 7.

Use of older versions of a Web browser is particularly common among Microsoft Internet Explorer users, so the Rumpus interface is also accessible by MSIE all the way back to version 5, although MSIE 7 or later is strongly recommended. (It is worth noting that use of MSIE versions older than 7 is rare these days.)

In most cases, use of an older browser only effects the appearance of the interface, although there are functional differences. The most obvious is the interface for uploading files. While modern browsers allow for drag and drop selection of multiple files, older browsers must use a standard file dialog to select files one at a time. Also, the file move operation requires drag and drop, and is only functional in the "modern" browsers listed above. Users of older browsers simply will not be able to move files from one folder to another.

Appearance Options

One of the best things about the Rumpus WFM is the amount of customization that is possible using a few simple controls. We strongly encourage you to spend a few minutes experimenting with the options available on the “Web Settings” and "WFM Appearance" windows so that the WFM integrates well with your company or organization and is easy for your clients to use.



Basic appearance options of the Web File Manager

Most of the options on the Appearance tab are fairly self-explanatory. To see the effects of any change, log into the WFM using a Web browser running on the server itself. After making a change, click the “Save Changes & Reload” button. Rumpus will save your changes and send a reload message to the front-most browser, quickly showing the effects of your updates.

Alternate Domains

In Rumpus, it is possible to define multiple “domains”, which allow you to customize the WFM interface displayed to each user. The terms “domain”, “appearance” and “interface” are used almost interchangeably in the section below. In Rumpus, we refer to this feature as “domains” due to the fact that the original use for this functionality was to provide for a distinct interface to be shown for different “virtual servers”, or alternate DNS server domain names. In fact, alternate domains can be displayed based on three different criteria:

Virtual Servers

Internet server names are assigned outside of Rumpus, via DNS, and multiple names can be assigned to a single IP address. Alternate Rumpus domains will be automatically displayed when a browser connects via a name matching the defined domain name in Rumpus. For example, a Rumpus server might have 3 domain names mapped via DNS: “files.acme.com”, “files.somecompany.com” and “uploads.acme.com”. One of these names will be considered the default domain, but two additional domains can be created in Rumpus, named exactly “files.somecompany.com” and “uploads.acme.com”. By creating these alternate domains in Rumpus, each of the 3 virtual servers can be customized in appearance independently.

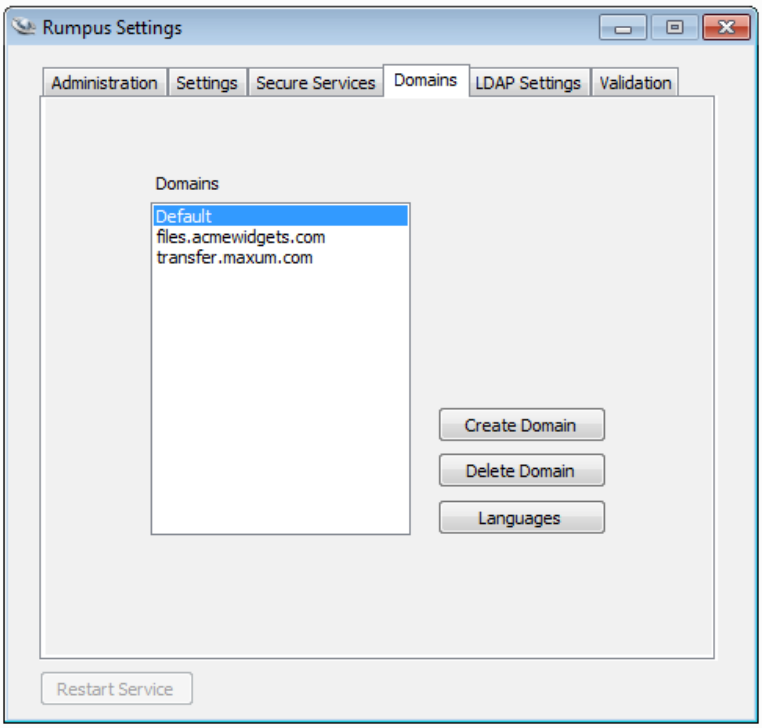
User Accounts

Alternate domains can also be applied to selected user accounts, allowing you to customize the WFM appearance for individual users. Select the domain to be displayed for each user from the “Alternate Domain” pop-up menu on the Define Users window.

User Selection

When users first connect to the server, it is also possible to allow users to select the WFM interface they would like to use. When the “Allow Users To Choose Domain” option is set on the “Options” tab of the Web Settings window, a pop-up menu will be presented listing each of the available domains, in addition to the usual name and password fields. The most common use of this feature is to allow users to select the language for the WFM interface. For example, if domains are created with the names “French” and “German” (in addition to the usual default domain), users would be able to select between those available languages when they login.

To define an alternate domain, open the "Settings" window and flip to the "Domains" tab.



Creating alternate domains

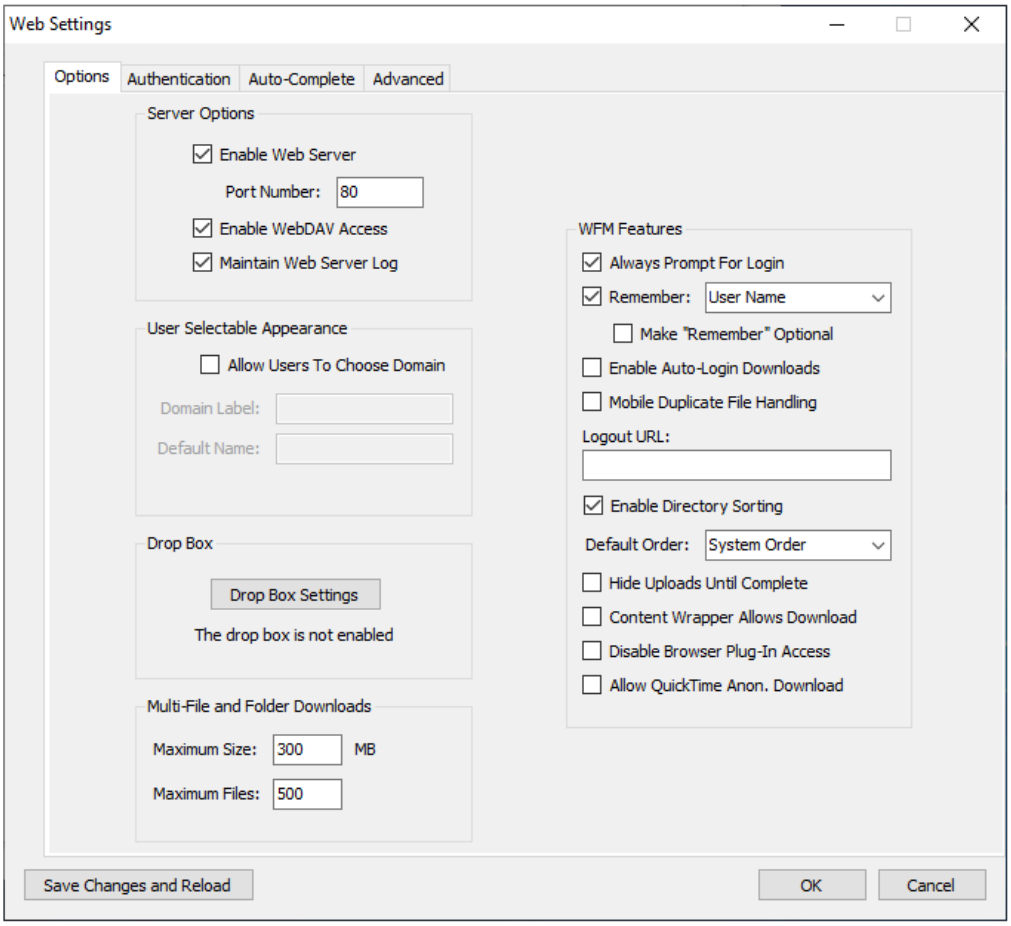
A domain, or alternate appearance, is defined by its name and a path to an alternate set of WFM templates. By using a different template set for each domain, you have complete control over every aspect of the interface, and can install different appearances (including languages) for each domain.

The choice of domain name depends on the reason for creating the alternate appearance. If the appearance will be used to provide a different look for an alternate server name (a virtual server), then set the domain name in Rumpus to the server name as set up in DNS. If the appearance will be user-selectable at login, choose the name you will want users to see when they select it from the pop-up menu. Finally, if the alternate appearance will be assigned to one or more user accounts for user-specific customization, choose any name system administrators will find easy to recognize.

Once the needed domains have been created, the WFM appearance can be customized for each, independently, by selecting the domain from the “Domain” pop-up menu at the top of the “WFM Appearance” window. When you select each domain from the menu, the appearance settings will change to reflect the selected domain, and any changes you make will be applied specifically to that domain.

Basic Options And Features

In addition to customizing the basic look of your WFM server, numerous options are also available that allow you to customize the features available to users. These features can be enabled or disabled on the Web Settings window, "Options" tab.



Web File Manager feature options

Notice that all of these options, and most others on the Web Settings window, are easy to change from one setting to another. Don't hesitate to experiment by checking the option check box or selecting a new choice from a pop-up menu. Each time you want to see the results of a change, click the "Save Changes & Reload" button. In most cases, you can see the results of your settings changes in just a few seconds. If you decide that the option isn't right for your server, changing it back is usually just as quick.

2-Factor Authentication

Everyone is familiar with the concept of supplying a password to gain access to some service on the Web. A password is essentially a secret that only the user knows, which they supply when logging in to prove they are who they claim to be. 2-factor authentication simply means that a second mechanism must also be used to confirm the person's identity.

With Rumpus 2-factor authentication enabled, users will need to supply a password and a personal identification number (PIN) in order to be granted access to the system. The PIN is sent at the user's request to their e-mail account. By entering both a password and a PIN, a user therefore confirms that they have the secret password *and* access to the e-mail account associated with their Rumpus user account. By confirming the user's identity in 2 different ways, security of the server is increased.

Requirements

Before enabling 2-factor authentication, you'll need to make sure that the Rumpus server is capable of sending an e-mail to ev

ery user account that will be accessing the system.

First, define an Event Notice to send the e-mail, configured with the needed SMTP settings to send yourself a test message. In other words, set the "Mail To" field of the Event Notice you your own e-mail address, for testing. When used in practice, Rumpus will automatically over-ride the specified Mail To address with the address of the intended recipient. On the Custom Message Body window, choose "Send 2-Factor PIN" from the Event Type menu to have Rumpus create a sample message, then customize the message as needed.

Next, make sure that the E-Mail Address field has been supplied for every user account on the User Accounts window. For sites with many users, this may be time-consuming, but it is just as essential as assigning user account passwords. Rumpus must know the e-mail address of every user so that it can use that e-mail account to confirm the user's identity.

Set-Up

To enable 2-factor authentication, open the Web Settings window and flip to the "Authentication" tab. Check the "Enable E-Mailed Access PIN" option and select the 2-factor PIN Event Notice from the Access PIN Notice list.

Remembering The PIN

Requesting a PIN, waiting for it to arrive, and transcribing it from the e-mail message to the login page isn't too difficult a process, but for frequent users, it can become time-consuming. To minimize the inconvenience, you may choose to have the PIN remembered in a browser cookie for a period of time. In this case, the user will only need to request a PIN periodically.

Note that when logging in without the need to request a new PIN, 2-factor authentication is still engaged. The PIN is stored by the user's local browser, at which point the 2nd factor becomes the fact that the user is connecting to the server from a known client. With that said, whether or not you require PIN authentication only periodically depends on the security requirements of your server or organization. To disable the feature of caching the PIN entirely, set the "PIN Re-Entry" number of days to "0", in which case, users will be required to request a PIN every time they log in.

Moving Files

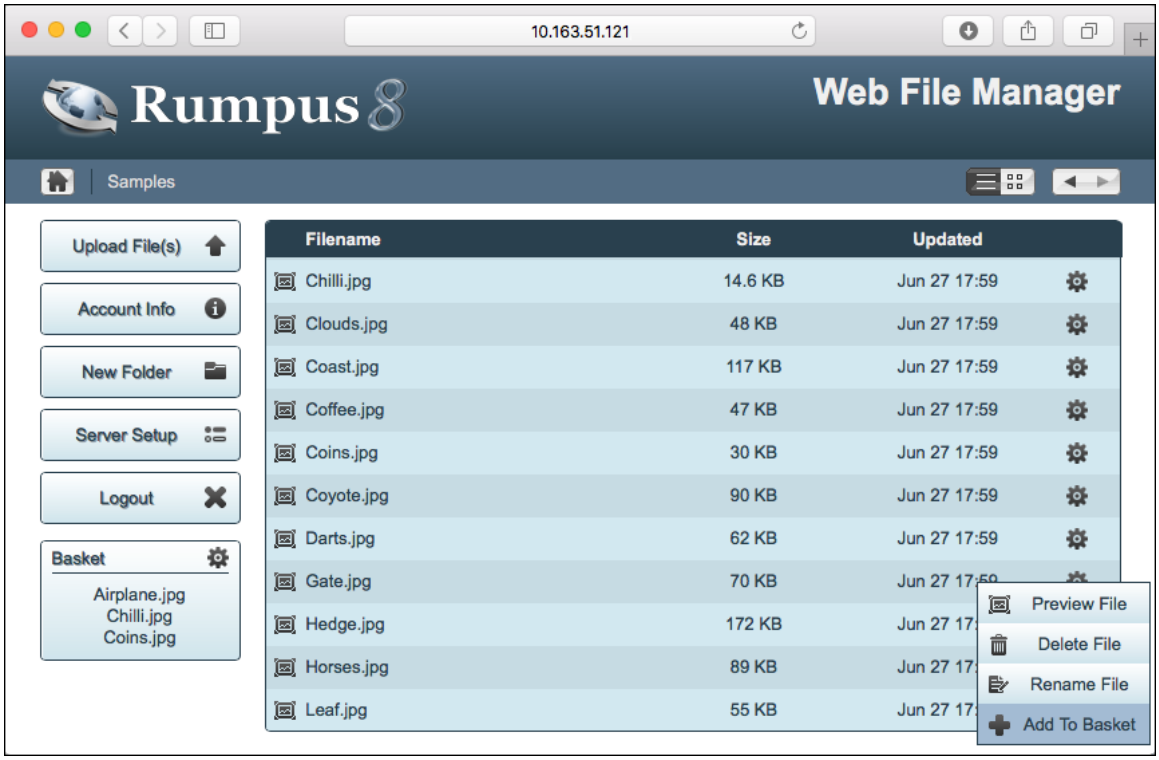
On the “WFM Appearance” window, “Listings” tab, enable the “Allow Files To Be Moved” option to allow users to move files from one folder to another.

To move a file, the user drags the file icon to the destination folder icon. Files can be moved “up” to the user’s home folder or a parent folder by dragging the file onto the appropriate element in the navigation bar. In “standard” directory list view, only the small file and folder icons are drag and drop-able. In thumbnail view, the entire thumbnail image of the file being moved can be dragged.

Important! Rumpus uses drag and drop functionality in modern Web browsers to implement the “file move” feature, so users of older browsers will not be able to move files. Browsers that adequately support drag and drop include Safari 7+, Google Chrome 26+, FireFox 16+ and Microsoft Internet Explorer 10+.

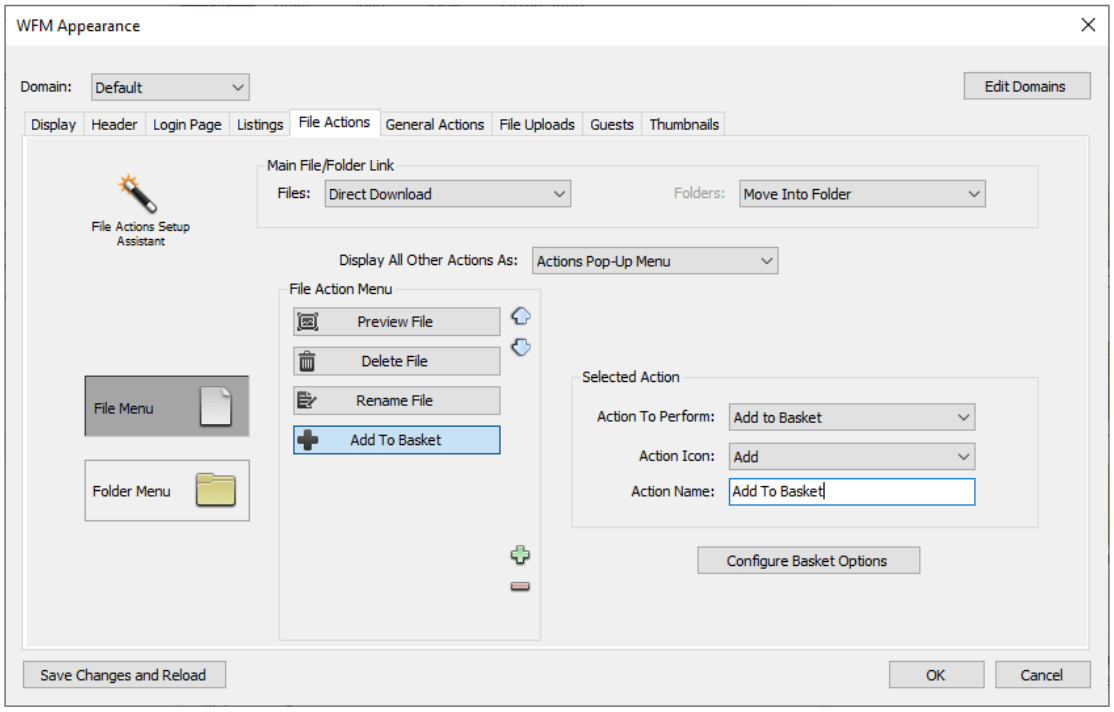
Baskets

The Rumpus "Basket" is a useful feature, especially for those who use the Drop Ship function extensively. In essence, the feature allows users create a collection of files and then process the collection in a single action. Users can move from folder to folder within their content area, adding files to the basket as they go. The basket can then be drop shipped in a single drop ship URL, moved to a set destination folder, etc. In the case of a drop shipment, when a basket of files is sent, the recipient accessing the drop ship URL sees each file sent and can view or download the files as needed.



In this example, the basket already contains the files "Airplane.jpg", "Chili.jpg" and "Coins.jpg", and "Horses.jpg" is about the be added to the basket. The user can then perform an action on the basket, such as drop shipping it's entire contents, by making a selection from the actions menu, represented by the gear icon in the basket box.

To enable the Basket, open the Web Settings window and flip to the "File Actions" tab. Select the File actions and click the add button to add a new action. Configure the new action (most importantly, the "Action To Perform" selection) as shown in the screen shot.

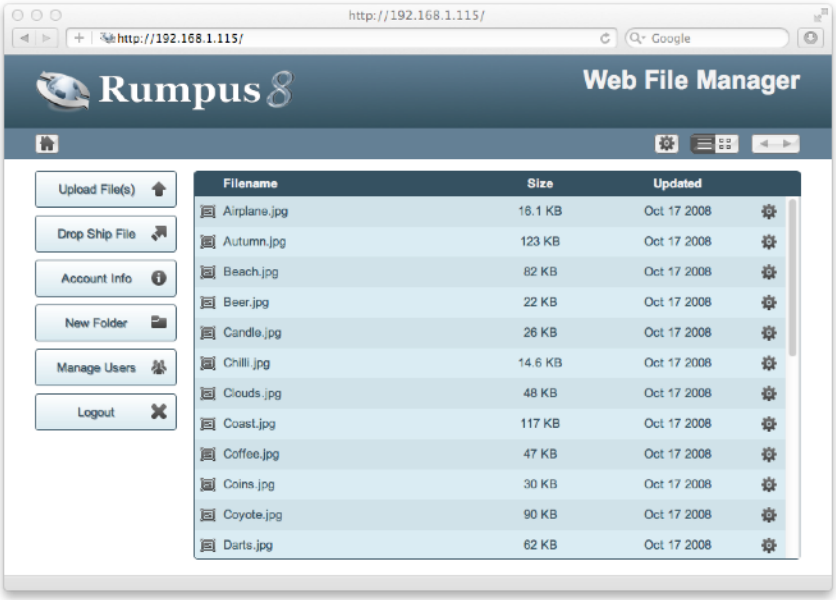


Notice that a button is made available for "Add To Basket" actions for configuring the behavior options for the basket function.

In the Web interface, users will now be able to add files to the basket, then download the entire basket, move all the files in the basket or drop ship the entire basket content in one action.

Thumbnail Listings

Consider a typical Rumpus WFM directory listing, as shown below.



A Web File Manager file listing in the default file view

Since this folder contains JPEG images, it might be more convenient for users if the listing were to display a thumbnail image for each file, providing a small version of the image contained in each file. Rumpus thumbnail listings allow you to display the folder in just that way.

A file listing in thumbnail view

To enable thumbnail listings, open the “WFM Appearance” window and flip to the “Thumbnails” tab, then choose either “Enable Thumbnails For Marked Folders” or “Display Thumbnail View For All Folders”.

The “Thumbnails” tab offers several options for controlling the appearance of the listing. For example, the “Thumbnail Width” and “Thumbnail Height” settings allow you to specify the size of each thumbnail image. The total size of the listing area will be the same as the standard line-by-line listing, so to control the total width of the list area, adjust one or more of the “Column Widths” on the “Listings” tab, each of which contribute to the overall width of the box.

Windows system functions are used to generate thumbnail images from native files, which means that the ability to generate a thumbnail from any given file type depends on the underlying OS running on the server. There are thousands of different types of files, and the ability to generate a thumbnail will depend on the system and the format of the content on your server.

Marking Thumbnail Folders

In cases where some, but not all, folders on your server need to be displayed as thumbnail listings, Rumpus administrative users can mark individual folders for display. On the “User Accounts” window, set the “Administrator” privilege for those accounts that need the ability to mark folders for thumbnail display. Assuming the “Enable Thumbnails For Marked Folders” option has been selected, administrators will then be provided with a “Thumbnail Actions” menu on the usual Rumpus directory listing page.

Administrators can use this menu to mark folders, unmark folders, or regenerate the thumbnail images (which can be useful when making changes to the image size options, necessitating the recreation of thumbnails which have already been created).

Quick Image Preview

As described above, thumbnail view directory listings are very useful for sites, or individual folders, which include graphic files or other visual media. For these types of files, it is often useful to view the image in a larger size than the tiny thumbnail shown in the listing, but without having to download the entire file. Quick Image Preview allows users to do just that, presenting a down-sized version of the image directly within the Web interface.

For example, typically when a user clicks a file, a pop-up menu is displayed, which includes options to view the file and download it. With QIP enabled, when the user chooses the view option, something like this is what they'll see:

A typical jpeg file displayed using Quick Image Preview

To close the preview, the user simply clicks the "x" close button.

Like thumbnail view directory listings, Rumpus relies on the server OS to generate the preview images. Rumpus uses the same image processing capabilities of the server, so all of the file types supported in thumbnail view will also be available as previews.

Movies can also be played directly in the browser using the QIP interface. When a video file is viewed the interface is similar, but the movie will always be played at its native resolution. (Resizing video files on the server isn't practical.)

Auto-Login URLs

At some point, you may have a need to allow a user to log in using a secure user account but bypass the login window. For example, you may wish to send a URL link to someone via e-mail, and have that link complete the login process and take the user immediately to the primary WFM directory listing page. This can be accomplished using a URL of the following form:

```
http://your.rumpus.server:port/?login=username:password
```

Of course, replace "your.rumpus.server" with the name or address of your Rumpus server, and "port" with the WFM port. Essentially, the link is simply the usual WFM access URL, as described above, with "?login=username:password" appended to it, where "username" and "password" represent the actual account name and password you would like the user logged in under.

Links can also direct the user to a specific folder or file, allowing you to send a URL that leads immediately to a file download or directing the user to a particular directory in the folder hierarchy. In this case, simply append the "?login=username:password" auto-login directive to the complete URL to the file, as in:

```
http://your.rumpus.server/folder/target.file?login=username:password
```

Obviously, there are security implications to consider when distributing URLs of this form. In particular, anyone that obtains the URL will be able to log in securely through that account, and the name and password are readily visible in plain text. When allowing users the ability to bypass the login process, consider whether using the anonymous user account wouldn't be a reasonable alternative. And if you do choose to use auto-login URLs, be very careful to restrict the login account as much as possible, and delete the account when it is no longer needed (or have Rumpus automatically expire it).

Instant Access Bookmarks

Instant access bookmarks allow users to generate a special URL that immediately resumes a previous session. They can be useful in several cases:

- Users can create a bookmark that immediately connects them to the server, bypassing login. In conjunction with HTML5 drag uploads, this means that a user could potentially upload multiple files with just a few clicks, simply clicking a bookmark button to log in, dragging the files into the browser window, and clicking "Upload".
- You can generate a URL and e-mail it to someone, granting them instant access to the Rumpus server by simply clicking the link. This use is similar to Drop Shipments or File Requests, except that instead of a simple interface for downloading or uploading a single file, the user gains access to the standard WFM interface.
- You can generate "Auto-Login URLs" that don't need to include the special "?login=" text or the user account name and password. For example, if you need to link users from your primary Web site to the Rumpus server, bypassing login, an Instant Access Bookmark can be used to generate the URL.

Important Security Note:

There are significant security implications involved in enabling Instant Access Bookmarks. The most obvious is that if a user creates a bookmark and adds it to their bookmarks page, and someone else gains access to that computer, that person may access the server without needing to authenticate. However, Instant Access Bookmarks are preferable to sending URLs that embed a username and password, as well as various other non-secure but common practices. Instant access bookmarks should be enabled only on servers where data security is not a major concern.

Instant access bookmarks can be enabled on the “General Actions” tab of the WFM Appearance window. To create an instant access bookmark, log in to the Web File Manager normally, then choose “Create Bookmark” from the Actions menu. Rumpus will generate the instant access URL and direct the browser to it. Users can then create a bookmark in the browser, or the URL can be copy/pasted from the browser’s address bar.

When the Rumpus server is accessed via instant access bookmark, the option to create a bookmark will not be presented. To create an instant access bookmark, a user must connect to the server and login normally.

File Search

Rumpus displays files hierarchically, with files displayed in directories (folders) which are navigated in much the same way as they are in a traditional file system. However, users can also choose to search for files by name.

First, search needs to be enabled, using the pop-up options menu on the "General Actions" tab of the WFM Appearance window. The available options include: "Disabled" and "For Filenames". Choose "For Filenames" to allow end users to search for text contained in filenames.

All searches are performed as a case-insensitive "contains" search, meaning that a match is found when the filename contains the search word specified, regardless of case. For example, a search word of "custom" would result in a response that includes filenames containing text such as "Custom" and "customizable". Users can specify multiple search words in a query, and choose between receiving a response where files contain either "any" or "all" of the search words. For example, a search phrase of "custom web interface" could result in a file list where files include all 3 search words, or any of the 3, depending on the user selection.

Searches are also restricted in scope to the folder in which the user currently resides, including sub-folders of that folder. For example, when a user first logs in and a directory listing of their top-level Home Folder is displayed, any search the user performs will be performed within the user's entire Home Folder. If the user moves down into a sub-folder and then performs another search, that search will be made only through files in that folder hierarchy.

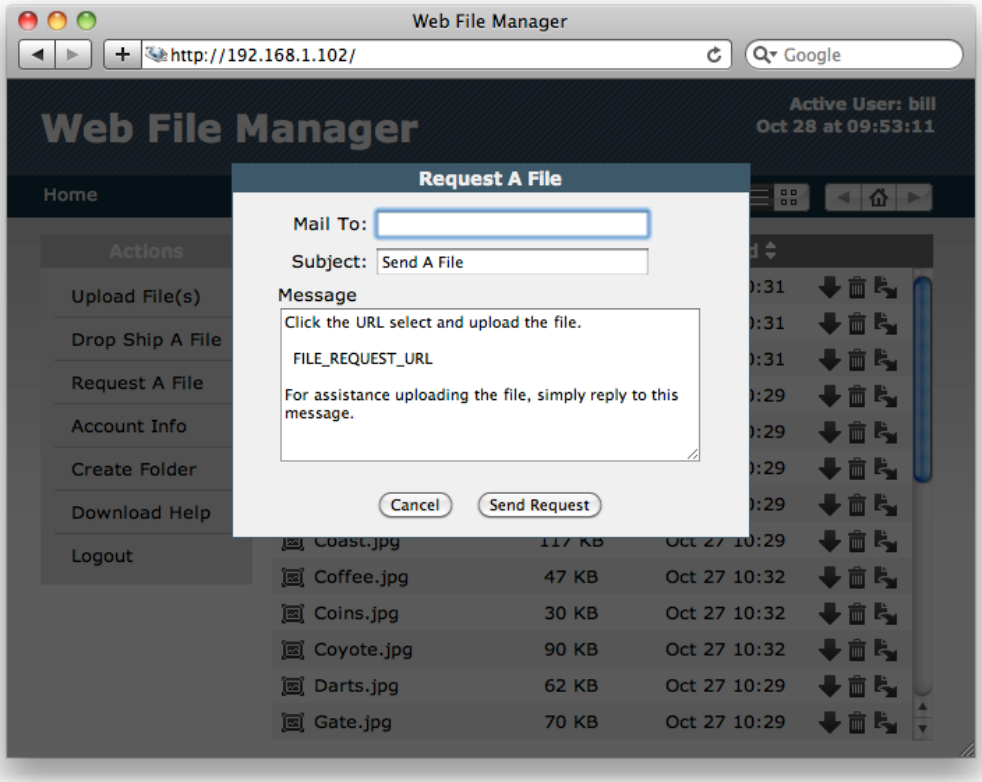
Search results are shown in a traditional Rumpus file list, with files linked normally. Users can return to the standard directory listing by clicking the folder name (or "Home") in the folder "breadcrumb" list.

File Requests

When a Rumpus user needs to send a large file to an outside person, Drop Shipping, described in the "Drop Shipping" article, is the ideal solution. However, the reverse case, where an outside person that doesn't normally have access to your Rumpus server needs to send a file to a known user, is also possible. In this case, Rumpus "File Requests" can be used to allow Rumpus users to give one-time file upload access to anyone they wish.

Transferring Files Via File Request

The process starts with the Rumpus user (the "requester") logging in the their Rumpus user account and navigating to the folder in which they would like to receive the file. Next, the user clicks the "Request A File" action link, which opens a dialog that looks something like this:



The File Request dialog box

The requester specifies the e-mail address of the person that will be sending the file, and can customize the message subject and message body as needed. When the user clicks "Send Request", Rumpus delivers an e-mail message to the specified address, which includes a unique link that will be used to send the file.

When the outside user (the "sender") receives the e-mail and clicks the send link, their local Web browser opens to a very simple page that prompts them to select the file and complete the upload. No login or extra work is necessary, and the interface shown to the sender is customized with your logo and other appearance options just like any other page in the Web File Manager. During the file selection and upload process, the user is considered a guest of the Rumpus user that requested the file. When the transfer is complete, the guest user is automatically logged out of Rumpus, and they can take no other action and access no other Rumpus services.

Additional data can also be collected from the sender, using an optional Upload Center form. For example, if local Rumpus users send file requests for artwork or other files associated with a job being performed, an Upload Center form prompting the sender to enter the job number and other information could be displayed on the file upload page.

Finally, an Event Notice is triggered which notifies the requester that the file upload has been completed. If an Upload Center form is used for requested file uploads, the Event Notice will typically be sent as an e-mail, and the data entered by the sender will be included in the message body.

Enabling And Configuring File Requests

To enable file requests, open the WFM Appearance window and flip to the "Guests" tab. Check the "Enable File Requests" box to enable or disable file requests. The number of days unused File Request URLs remain active, and whether or not File Request URLs can be used only one or repeatedly until they expire, can also be selected.

If you would like to have an Upload Center form presented to senders when uploading the requested file, select the form from the "Upload Center Form" pop-up menu (see the "Upload Center" article for details). Finally, select an Event Notice to be triggered after the requested file has been uploaded.

Specifying an Event Notice to be triggered is, in most cases, particularly important. An uploaded notice trigger isn't technically required, but without it, the Rumpus user who requests the file will not be notified when the file has been uploaded. If the Event Notice is an e-mail notice, Rumpus will automatically replace the "Mail To" address with the Rumpus user's e-mail address, as specified on the Define Users window.

Each Rumpus user who will be given the ability to request files needs to be granted the privilege. Open the "User Accounts" window and select the "Send File Requests" privilege for each user account.

Important! Be sure to also set the e-mail address (on the "User Info" tab of the User Accounts window) for users that will send File Requests. The user account e-mail address is used as the "reply to" address when sending the message to the sender and as the "mail to" address when Rumpus sends the Event Notice after the file has been received.

Well-Known Locations

Web servers sometimes need to be able to deliver standardized content, usually used by automated systems or scanners, that help define the server's capabilities or ownership. A good example is a file provided to you by an SSL Certificate Signing Authority, which serves to prove that you control the content of your server.

The proper way for clients to access such content is via URL with the prefix "/.well-known/". Should you need to put content on your server so that clients (including automated scanners) can access it without the need to log in, Rumpus includes a "well-known" content folder feature.

In Rumpus, choose "Open Config Folder" from the "File" menu to access the Rumpus config folder at "/usr/local/Rumpus/". In the config folder, create a folder named exactly "well-known", which enables the well-known location feature. Note that URLs that access this content will include a period, as in ".well-known", but the period is not necessary and should not be included in the folder name.

Any file placed within the "well-known" folder will be accessible to outside clients via the "/.well-known/" prefix. For example, if you were to place a file named "example.txt" in the well-known folder, it would be accessible to all clients via the URL:

> http://your.server.address/.well-known/example.txt

Importantly, if you need to add accessible content within a specific folder structure, you can create that folder structure within the well-known folder. For example, if the client needs that content to be accessible via the URL:

> http://your.server.address/.well-known/validation/example.txt

you would create a folder named "validation" within the well-known folder, and then put the file "example.txt" in that folder.

Customizing The WFM Interface

The WFM interface is actually a series of standard HTML pages, embedded with special tags that tell Rumpus where to include dynamic information (such as folder listings). These pages can be edited, if you wish, to include help information, alter the WFM behavior, or to simply change the look of the WFM to better integrate with an existing Web site.

Important! Note that future versions of Rumpus are likely to require alterations in the WFM template set. In general, when upgrading Rumpus, older template sets will continue to work as expected, but new features introduced in the Web File Manager often require corresponding updates to the template files. We strongly recommend that when making changes the the WFM templates, you make a note of the changes made so that they can be easily reproduced in the future. If your template customizations are extensive, taking advantage of future version updates may be difficult.

The WFM template pages are all stored in the “WFM Templates” folder at:

C:\Rumpus\WFMTemplates\

The significant files that are included in the template folder(s) are:

wfm.css

The basic appearance of the WFM is defined largely through CSS. Most WFM template files link this file as the style sheet definition.

Login.html

When users first connect to the server, this page is used to display the username/password authentication form.

Listing.html

This is the primary interface page for the WFM. It displays folder listings, allows file uploads and downloads, includes the user account information, etc.

NoListing.html

Usually, this is a copy of the "Listing.html" page, with the folder listing section removed. It is displayed in place of the "Listing.html" page when the user does not have "View Directory" privileges for the current folder.

Message.html

Rumpus will have a number of occasions to display various status messages. This page is used for all simple cases where a message needs to be presented. For example, the "Upload Complete" message displayed after a file upload is sent using this page format.

Logout.html

When the “Logout” link is clicked, this page is sent to the browser.

DownloadPage.html

The “Download Page” is displayed only when the “Download Page” option is selected for either the filename or alternate link settings, and the user clicks the download link in the directory listing. In this case, this page is served instead of Rumpus delivering the requested file directly.

HelpPage.html

This page is used to provide WFM usage help to new users.

ContentWrap.html

This page acts as an example of how to embed content within a WFM template page. When either the filename or alternate link is set to use the “Content Wrapper” option, and a user clicks the link, the ContentWrap.html page is served. This page then embeds that file originally chosen by the user. Different media types can be presented in unique ways by overriding the default ContentWrap.html page for specific file types. Use the File Types window to specify alternate content wrapper pages for the various types of files available on your server.

UploadStarting.html

When progress indicator pop-up windows are enabled, this page is displayed in the pop-up window when initially opened. Upload statistics won’t be accurate until a reasonable portion of the uploaded file (64k or so) has been received, so this page is shown while the transfer begins.

UploadProgInd.html

This is the primary page displayed in the progress indicator pop-up window, and includes transfer statistics which are reloaded on regular intervals to let the user know the upload is proceeding.

UploadComplete.html

When a file upload completes, this page is displayed in the main browser window. When progress indicators are used, a javascript in this page closes the progress pop-up window.

RumpusStat.html

This page displays the Rumpus server statistics to users with "administration" privileges when server monitoring is enabled. The page is complex, as it performs dynamic updates using XML requests of your Rumpus server, and is not seen by external users, so we don't recommend that the page be altered.

Referencing Additional Files

The Web File Manager also acts as a standard, though very simple, Web server. Files placed in the "WFMTemplates" folder will be served as they would from any Web server. So, for example, images used in your modified WFM templates can be placed in the WFMTemplates folder and linked into the page using the standard "IMG" tag.

Be sure to make all URL references to additional files "root-relative", which start the URL with a slash ("/") in the hypertext reference. As the user dives into folders and sub-folders, the browser URL will reflect the folder being viewed, not the WFM template file. You therefore can't use URLs that are relative to the template file. Hypertext references must instead be relative to the server's root folder, which, in the case of the Rumpus WFM, is the WFMTemplates folder.

WFM Dynamic Content Tags

Within template pages, a variety of tags are used to insert and process the content being presented. In other words, tags tell Rumpus where to place the directory listing itself, user information, and other variable content within the templates. These tags, which all begin with "WEBFILES", fall into two categories: those that simply insert content into the template page, and those that conditionally include or exclude content as needed.

Insertion Tags

<WEBFILES_DATE>

Inserts the current date.

<WEBFILES_TIME>

Inserts the current time.

<WEBFILES_HEADER>

Inserts a dynamically created page header.

<WEBFILES_HEADER_CSS>

Inserts a dynamically created page header specifically for use in CSS-formatted pages.

<WEBFILES_HOST>

Inserts the hostname used by the client to connect to the server.

<WEBFILES_LOGINLINK>

Inserts a link to the Rumpus login page.

<WEBFILES_LOGOUTLINK>

Inserts a link to the Rumpus logout page.

<WEBFILES_MESSAGE>

Primarily intended for use on the "message.html" template, inserts a status message.

<WEBFILES_PARENTDIR>

Inserts the path to the current folder.

<WEBFILES_PATH>

Inserts a formatted, hyperlinked path to the current folder.

<WEBFILES_THISFILENAME>

Inserts the name of the file being processed (for deletion, for example).

<WEBFILES_THISURL>

The URL currently being processed.

<WEBFILES_HOME_URL>

Insert a formatted URL to the top level of the server.

<WEBFILES_BACKLINK "EnabledText" "DisabledText">

Inserts a hypertext link to move the user up one folder in the hierarchy. If the user can move up, the "EnabledText" (which may be an image reference) is inserted as the linked text. If not (such as when the user is in their top-level home folder), the "DisabledText" is inserted.

<WEBFILES_FORWARDLINK "EnabledText" "DisabledText">

Inserts a hypertext link to move back down to a previously visited folder lower in the directory hierarchy. If the user can move down, the "EnabledText" (which may be an image reference) is inserted as the linked text. If not (such as when the user has not accessed folders lower than the current directory), the "DisabledText" is inserted.

<WEBFILES_UPLOAD_CENTER>

Insert the Upload Center input form specified for the active user account.

<WEBFILES_REQUIRED_FIELD_CHECK>

Insert javascript to verify field contents for Upload Center forms.

<WEBFILES_VAR VariableName>

Numerous configuration, user account, and file transfer variables are also available for inclusion in the page being sent to the browser. For example, to insert the font size chosen in Rumpus for text in the WFM, the token "<WEBFILES_VAR FileSize>" would be used.

The variables available are:

BGColor	The background color for WFM pages.
TextColor	The selected color for WFM text.
LinkColor	The text color for hypertext links.
Hilite1	The primary highlight color, as selected in the Rumpus control application.
Hilite2	The secondary highlight color, as selected in the Rumpus control application.
Hilite3	The alternate highlight color, as selected in the Rumpus control application, used for alternating lines in the file listing table.
FontFace	The WFM font, as selected in the Rumpus control application.
FontSize	The WFM font size, as selected in the Rumpus control application.
LinkStyle	The text style for hypertext links.
HoverStyle	The text style selected for use when the cursor moves over a hypertext link, such as a file name in the file listing.
Title	The WFM title, as specified in the Rumpus control application.
Logo	The logo filename, as specified in the Rumpus control application.
LogoLink	If the logo filename is specified, an image tag that displays the logo.
Username	The current user account name.
Password	The current user password, as supplied at login.
UserLogins	The number of times the current user account has been used to log in to the server.
UserBytesUp	The amount of raw data uploaded over the history of the current user account.
UserBytesDown	The amount of raw data downloaded over the history of the current user account.
UserFilesUp	The number of files uploaded over the history of the current user account.

UserFilesDown	The number of files downloaded over the history of the current user account.
PIWindWidth	For use in the ProgressIndicator page, a reasonable width for the progress indicator window based on the selected font size.
PIWindHeight	For use in the ProgressIndicator page, a reasonable height for the progress indicator window based on the selected font size.
Filename	For use in the ProgressIndicator page, the name of the file being transferred.
FileSize	For use in the ProgressIndicator page, the size of the file being transferred.
PercentComplete	For use in the ProgressIndicator page, the percentage of data transfer completed so far.
Ratio300	For use in the ProgressIndicator page, this value represents the completed file transfer amount as a value from 1 to 300.
BytesSent	For use in the ProgressIndicator page, the number of bytes sent so far in the current transfer.
ElapsedTime	For use in the ProgressIndicator page, the time elapsed since the transfer was started.
EstimatedTime	For use in the ProgressIndicator page, an approximation of the time remaining in the transfer based on the transfer rate achieved so far.

<WEBFILES_LIST_LM "TableControl1" "TableControl2" "DeleteText">

This tag is special. It may be used only once, and only on the "Listing.html" page. It inserts the folder listing for the current folder.

"TableControl1" and "TableControl2" are extra parameters that will be placed in the Table Row HTML command for each line of the folder listing. The extra formatting text will be inserted alternately on each line of the listing. These parameters are usually left blank, in which case Rumpus will automatically alternate row colors using the highlight color values specified in the Rumpus control application. A few special keywords are available for both the TableControl values. Either parameter may be set to “H1”, “H2” or “H3” to have Rumpus use the Highlight1, Highlight2 or Highlight3 color values for the row background color. Alternatively, you may specify “MO” (Mouse Over) for both parameters, in which case Rumpus will set up the rows for the mouseover effect. In this case, the “Highlight2” color will be used as the background for each table row, but will change to “Highlight3” as the user’s pointer moves over it.

The “DeleteText” parameter allows you to specify the text displayed in the “delete” link of folder listings. The default is “del”, but the text can be changed to any word, or even an HTML image tag, up to 90 characters long.

If you prefer to have the directory listing displayed without the last modified date of each file and folder, remove the “_LM” portion of the tag, as in:

```
<WEBFILES_LIST “H2” “H3” “[ del ]”>
```

The token can also be written as “WEBFILES_LIST_CSS”, in which case in-line formatting in the table itself is minimized so that the display of each row is dictated by a style sheet embedded in the listing page.

Condition Tags

Condition tags include or exclude a block of text based on whether or not some condition is met. For example, the “WEBFILES_ANONYMOUS_USER” tag will include the specified text when the active user is logged in anonymously. The text included is specified between the tag itself and a matching end tag, which is the same as the opening tag, with the addition of a leading slash (“/”).

<WEBFILES_ANONYMOUS_USER> ... </WEBFILES_ANONYMOUS_USER>

Include the specified text when the active user is logged in anonymously.

<WEBFILES_ANONYMOUS_WITH_ANY> ... </WEBFILES_ANONYMOUS_WITH_ANY>

Include the specified text when the anonymous user account permits login with a password.

<WEBFILES_ANONYMOUS_WITH_EMAIL> ... </WEBFILES_ANONYMOUS_WITH_EMAIL>

Include the specified text when anonymous users may log in by specifying their e-mail address as the password.

<WEBFILES_SECURE_USER> ... </WEBFILES_SECURE_USER>

Include the specified text when the active user is logged in using a secure user account.

<WEBFILES_ADMIN_USER> ... </WEBFILES_ADMIN_USER>

Include the specified text when the active user has administration privileges.

<WEBFILES_STATS_USER> ... </WEBFILES_STATS_USER>

Include the specified text when the active user has the ability to review basic server statistics.

<WEBFILES_BAD_PASSWORD> ... </WEBFILES_BAD_PASSWORD>

Used on the login page, include the specified text when the user has previously entered an incorrect password.

<WEBFILES_GOOD_PASSWORD> ... </WEBFILES_GOOD_PASSWORD>

Used on the login page, include the specified text when the user has not previously entered an incorrect password.

<WEBFILES_DIRSORT> ... </WEBFILES_DIRSORT>

Include the specified text when directory sorting is enabled.

<WEBFILES_DOWNLOADLINKS> ... </WEBFILES_DOWNLOADLINKS>

Include the specified text when the download links option is enabled.

<WEBFILES_NEW_FOLDER_LINK> ... </WEBFILES_NEW_FOLDER_LINK>

Include the specified text when the user has permission to create new folders in the currently selected folder.

<WEBFILES_ACCOUNT_INFO> ... </WEBFILES_ACCOUNT_INFO>

Include the specified text when the “Include User Account Stats” option is enabled.

<WEBFILES_PASSWORD_CHANGES> ... </WEBFILES_PASSWORD_CHANGES>

Include the specified text when users are permitted to change their own passwords.

<WEBFILES_SEND_PASSWORDS> ... </WEBFILES_SEND_PASSWORDS>

Include the specified text when forgotten password lookups are enabled.

<WEBFILES_FILE_ICONS> ... </WEBFILES_FILE_ICONS>

Include the specified text when the "Enable File/Folder Icons" option is enabled.

<WEBFILES_UPLOAD_FORM> ... </WEBFILES_UPLOAD_FORM>

Include the specified text when the active user has permission to upload files to the currently selected folder.

<WEBFILES_NO_UPLOAD_FORM> ... </WEBFILES_NO_UPLOAD_FORM>

Include the specified text when the active user does not have permission to upload files to the currently selected folder.

The ability to modify the look of the WFM is an important feature of Rumpus's HTTP file management capability. However, the HTML formatting needs to remain consistent with the dynamic information inserted by Rumpus, or problems will occur. If you change the WFM template pages, be sure to start with the default files, and make small, incremental changes to the formatting. Also, remember to make frequent backups of your work, so that if something goes wrong you can return to a working template easily. When all else fails, you can always return to the default template set by clicking the "Appearance & Language" button on the Web Settings window, using that function to reinstall a fresh set of templates.