

Rumpus FileWatch

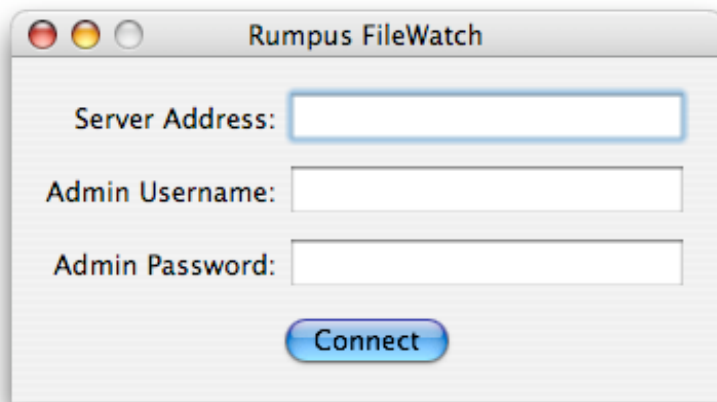
Monitoring user activity, file transfers, and exchanging files with your users.

Rumpus FileWatch is a supplementary application run on your own Mac desktop, in conjunction with your Rumpus file sharing server, that allows you to monitor outside user activity and recently uploaded and downloaded files. It also provides you with an easy way to access files that have been uploaded to the server and to “drop ship” files to anyone, right from your desktop, complete with automatic e-mail notification to the end user for file pickup.

This article primarily describes basic FileWatch use as it applies to any permitted local user, so we’ll begin with an overview of how to use the FileWatch client. Server administrators interested in enabling FileWatch on their Rumpus server and managing access may wish to start with the “Setup and Administration” section later in this article.

Connecting To The Rumpus Server

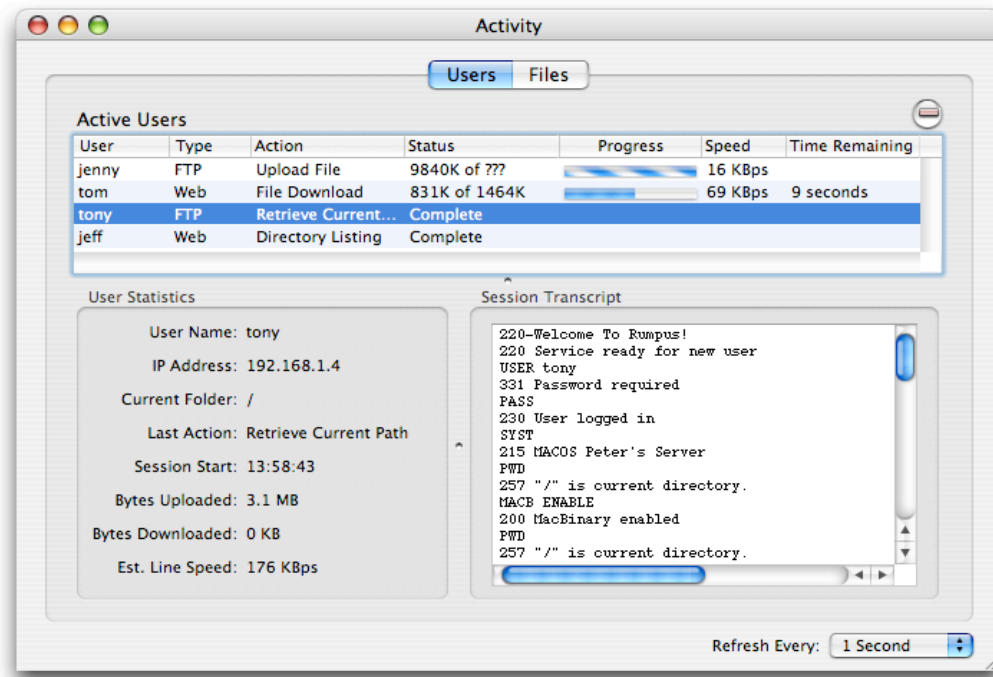
Once started, FileWatch will first prompt you for the server address and your account name and password, as shown here.



When connecting to a Rumpus server running on the same local network as your desktop Mac, be sure to supply the local IP address of the server. In the “Admin Username/Password” fields, supply your Rumpus administrator user account name and password. Finally, click “Connect” to log in to the Rumpus server and begin the session.

Monitoring User Activity

FileWatch consists of a single tabbed window. The first tab, “Users” displays a table listing all currently active user sessions, as well as detail areas to provide additional information about any selected account.



In the example shown above, four remote users are currently logged in to the Rumpus server. According to the “Type” column in the user list, two of these, Jenny and Tony, are logged in via FTP, while Tom and Jeff are logged in using a Web browser.

The “Action” column displays the last action taken by the user, while “Status” reflects the result or ongoing status of that action. Here, Jenny and Tom are actively transferring files, and the Status column reflects how much of the file data has been sent, along with the expected size of the file, when possible. (In the case of FTP file uploads, the size of the file being sent is not known by the server, but the total file size is usually displayed in all other cases.)

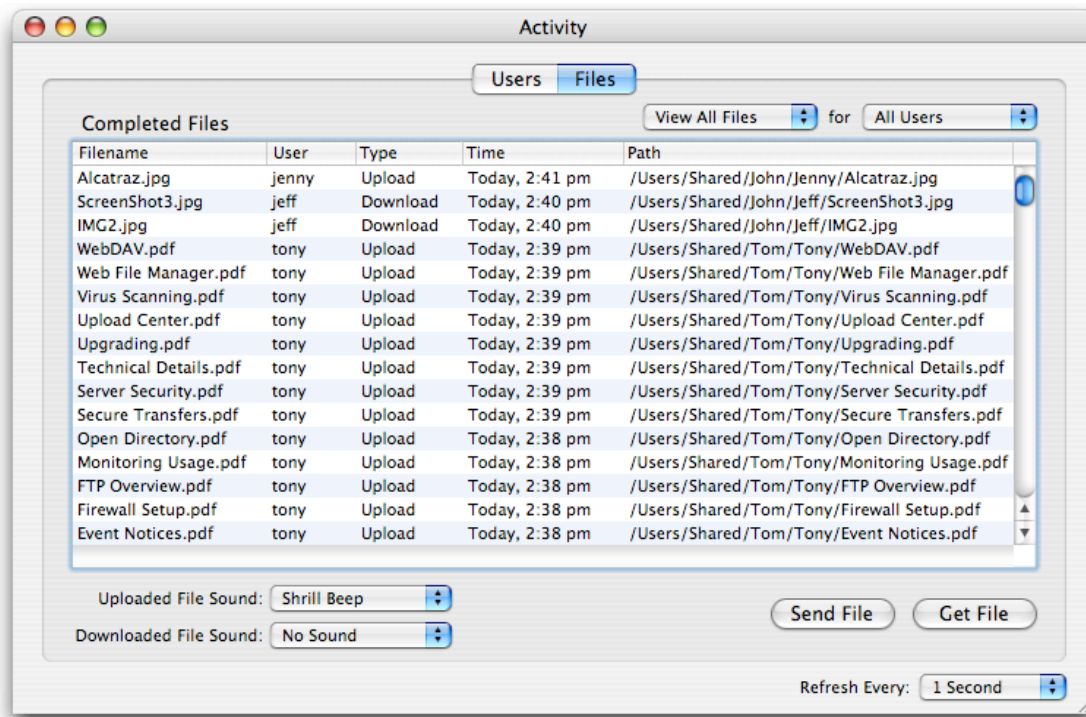
For active transfers, a progress indicator, estimated transfer speed, and time remaining are also shown. Each of these elements are estimated based on the data transfer rate of the portion of the transfer already completed. The actual time remaining, for example, may vary depending on conditions.

To review additional session statistics, select any listed session in the table. The user’s remote IP address, session start time, and other basic statistics are shown in the “User Statistics” box. Please note that the “Est. Line Speed”, like “Time Remaining”, is an estimate based on the current and past file transfers completed during the session. If either your Internet connection or that of the client is being shared by other Rumpus users or other services, the estimated line speed may indicate expected transfer rates well below the maximum possible for the connection.

Finally, the Session Transcript displays the complete record of activity for the active user session. This takes the form of an FTP session transcript, or for Web and WebDAV users, a summary of each action taken by the user. If the recording of session transcripts has been disabled in Rumpus, the session transcript will not be available.

Viewing Recent File Transfers

Flipping to the “Files” tab reveals another table, this one displaying recently transferred files. The filename, user that transferred the file, transfer type (upload or download), transfer time and full path as the file resides on the server is displayed.



The list can be filtered using the pop-up menus just above the list. These menus allow you to view only uploaded or downloaded files or only by a particular user, as needed.

File Upload/Download Alarms

If you like, Rumpus can sound an alarm when new files are added to the list. Simply choose the sound you would like played when a new file is either uploaded or downloaded from the appropriate pop-up menu just below the file list. It is important to note that the warning sound will only be played when a new file is added to the list, as controlled by the file type and user account filter. For example, if you have set the file display filter so that only uploaded files by the user “Tom” are shown, the warning sound will only be played when Tom uploads a file to the server.

To have a warning sound played for all file uploads, be sure to leave the filter set so that files are displayed for “All Users”. If, however, you are waiting for a file from a particular person, you can set the filter to display files only for that user, and the sound will play only when that person sends a file.

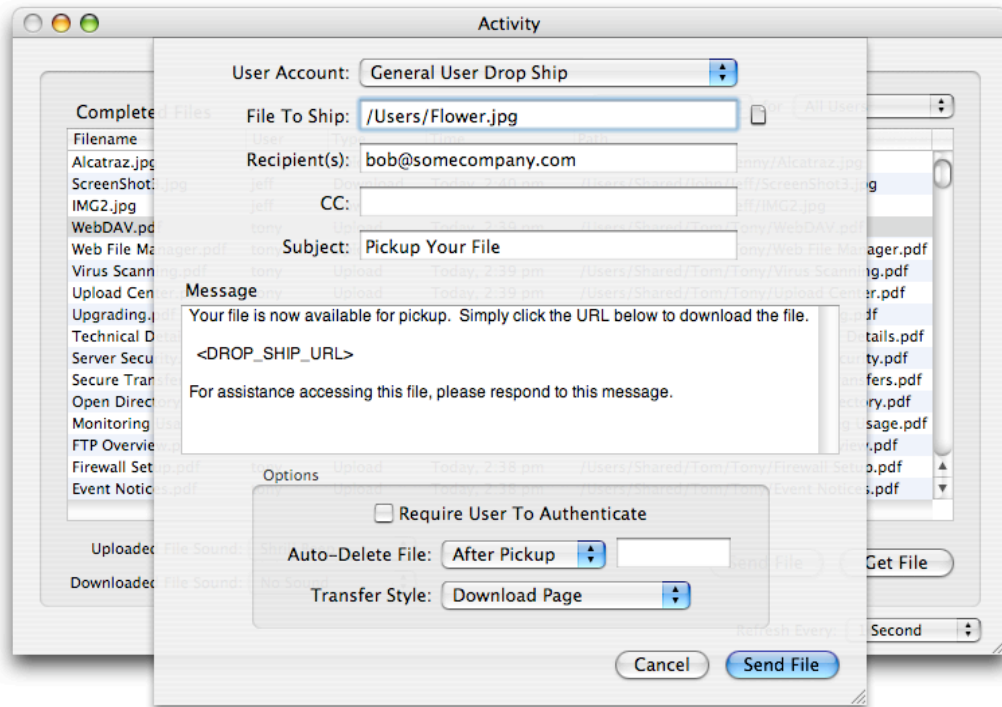
Retrieving Files From The Server

When a remote user uploads a file to the Rumpus server, it's very often necessary to retrieve a copy of the file to your own Mac. With FileWatch, this is easy; just select the file from the list and click the “Get File” button. The standard Mac “Save File” sheet will drop down, and you can save the file to any location on your local computer you like. Alternately, grab the file (click and hold on the entry in the file list) and drag it to the desktop or any folder open on your desktop. The file will then be copied to your computer automatically.

Drop Shipping Files To End Users

Drop shipping files is essentially an alternative to sending files as attachments to an e-mail message. When you drop ship a file, the file is posted to the Rumpus server, and an e-mail message is sent to the intended recipient. The e-mail includes a link, which the user can then use to download the file automatically. You can drop ship files to existing Rumpus users, or even to people that don't have a Rumpus user account. You can require that users supply their Rumpus account name and password to retrieve the file, or be given access to the file without authentication. You can also add comments to the message body, have the file automatically deleted after it is picked up, and control what the user sees when they access the file.

Drop shipping is initiated either by clicking the “Send File” button, or by dragging the file you wish to send into the file list. If you click “Send File”, a standard Mac “Choose File” sheet will be displayed, allowing you to select the file to send. If the file is dragged into the list, the “Drop Ship” sheet drops down immediately.



To have the file sent using an existing Rumpus user account, choose the account name from the “User Account” pop-up menu. When you choose a specific user account, the file will be placed into that user’s Home Folder, so that it is visible when they log in normally to the Rumpus server. If the file is being sent to someone that doesn’t already have a Rumpus user account, or if you want to send the file without having it added to a user’s normal Rumpus Home Folder, choose “General User Drop Ship”.

The “File To Ship” displays the file you are sending. The “Choose File” icon next to the field allows you to select a different file to send, using the standard Mac choose file sheet.

Next, enter the e-mail address of the person that will receive the file. Multiple people can be specified by entering each e-mail address, separated by commas. You may also “CC” additional recipients, if needed.

The e-mail message subject and message body can also be customized. In the message body, be sure to leave the “<DROP_SHIP_URL>” token in tact. Text can be added or customized around this token, but the token is necessary as it represents the link to the file, which will be generated automatically by Rumpus when the message is sent.

Additional drop shipping options are also available. If a specific user account has been selected to post the file into, you may require that the user enter their name and password after clicking the drop ship link in the message body. In other words, by checking the “Require User To

Authenticate” box, the user will be presented with the usual Rumpus login page when they click the link in the the e-mail message. Once they enter their name and password, the file transfer will then begin automatically.

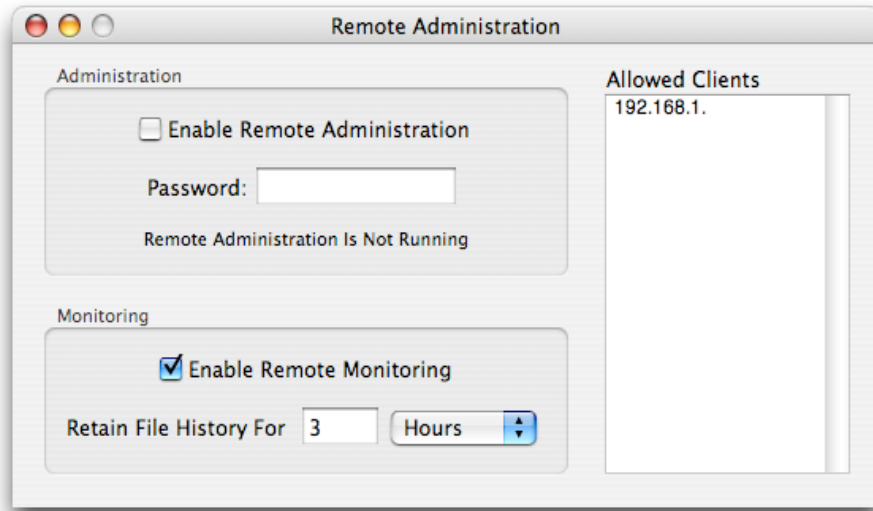
Drop shipped files can be deleted automatically after a set period of time. Note that if you choose “After Pickup”, the file will be deleted immediately after the user first downloads the file. In this case, the link sent to the user will work only once, and thereafter will become invalid.

The last option allows you to control how the browser will behave when the drop ship link is clicked. A “Simple Download” will cause the browser to load the file and process it directly. In this case, most Web browsers will display images, play sounds or movies, or otherwise present the content in the browser window, if possible. Other content types will likely be downloaded to the user’s computer, depending on the browser. Choosing “Download Page” will display a page to the user stating that the download is in progress, and the file will then be delivered. If you choose “Content Wrapper”, the drop shipped file will be displayed embedded within a formatted Web page, as set up in Rumpus.

When you click “Send File”, the file will be posted to the Rumpus server, and the e-mail will be sent. A status sheet will be displayed, keeping you informed of the progress, and displaying the automatically generated pickup URL, once the file is ready for pickup.

Setup and Administration

To allow FileWatch access, Rumpus remote monitoring first needs to be enabled. On the server, open the “Remote Admin” window, specify the “Allowed Clients” list, and check the “Enable Remote Monitoring” checkbox. To allow anyone on the local network to login via FileWatch (with an appropriate administration user account name and password), add the subnet to the Allowed Clients list by specifying only the first 1, 2 or 3 octets of the IP address range. For example, valid entries include “192.”, “192.168.1.”, “10.” and “10.0.1.”



Once remote monitoring is enabled, users on allowed addresses or subnets will be able to login via FileWatch using their Rumpus administrator user account. So, to give yourself or others the ability to use FileWatch, open the Define Users window and enable the “Administrator Access” option for whichever user accounts need FileWatch access.

You may also choose to enable session transcripts, by checking the “Record Session Transcripts” checkbox on the “Logs” tab of the FTP Settings window. The option is entirely optional, but when it is disabled, the “Session Transcript” display in FileWatch will remain blank.

Important Notes

Administrator Groups

When monitoring activity and transfers via FileWatch, only activity performed by users whose Home Folder falls within the administrator’s own Home Folder will be displayed. For example, if the person using FileWatch has a Home Folder of “/Users/Shared/GroupA/”, then FileWatch will display user activity and file transfers for remote users whose Home Folder is set to that same folder, or some folder within it.

By displaying only activity which falls within the administrator’s Home Folder, FileWatch allows different people within your organization to view and access only the files they need. Essentially, it allows you to create groups of users and control which local administrator is able to monitor each group. Administration accounts with a Home Folder of “ROOT” will always be able to monitor all server activity and view and access all file transfers.

Mail Settings

When users drop ship files, Rumpus FileWatch needs to send an e-mail message to the recipient. It does this using the Mail Server Defaults set on the Preferences tab of the FTP Settings window. The “Web Hostname” on the same tab is also required in order for FileWatch to build a proper URL to the server.

Auto-Deletion of Files

Drop shipped files are tracked in an internal Rumpus database until they expire. To ensure that the database isn't choked with forgotten files, all drop shipped files must be automatically deleted. The expiration period for drop shipped files can be set when the file is sent, to a maximum of 1 month. To post files for permanent access by users, upload the file through normal Rumpus client access. Note that if files marked for deletion “After Pickup” will automatically be removed after 1 week, if not downloaded sooner.

Preferences

Rumpus FileWatch uses and maintains preference settings both on the Rumpus server and the local Mac. Settings that are technical or apply to the Rumpus service as a whole, such as mail server preferences, user account options, etc. are shared among all FileWatch users via settings defined in the Rumpus control application. Other options, such as the login server address and administrator username, and various drop ship mail settings, are maintained on the Mac on which FileWatch is run, allowing individual administrators to maintain default settings independently.