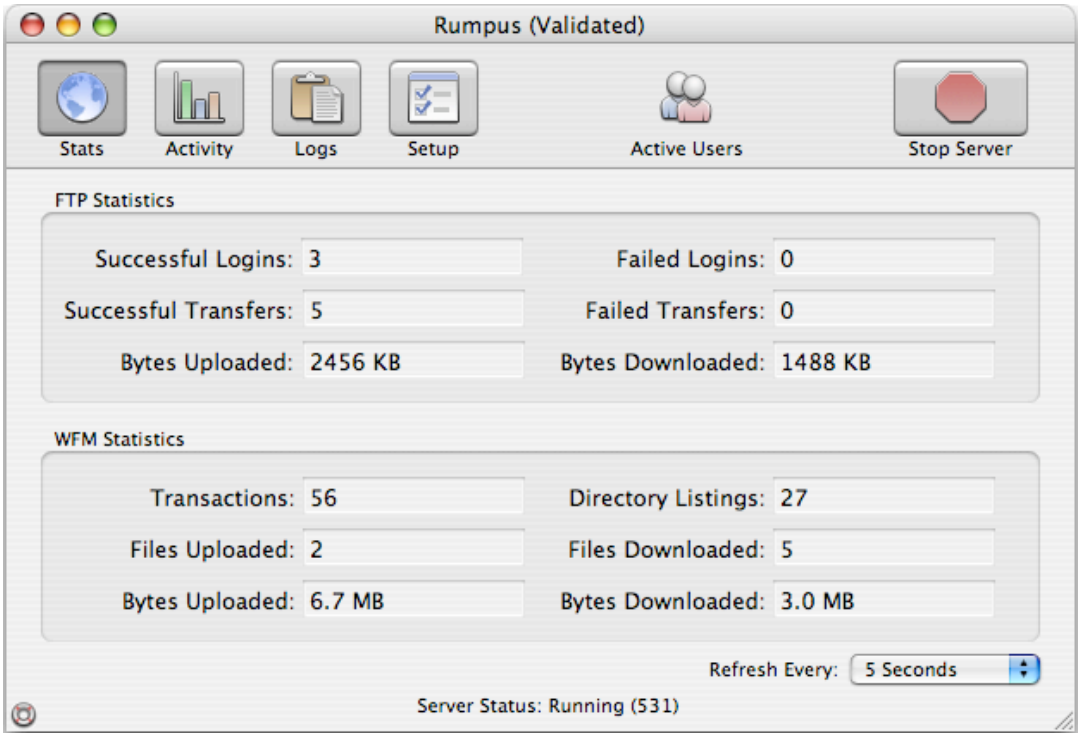
Monitoring Server Use

Using log files and activity reports to see who has been using your server, and what they have been doing.

Whether you are simply curious about who is currently using your server, need to watch for unauthorized access, or wish to review user activity, Rumpus will provide you with the information you need. The Rumpus control application displays basic statistics, information about active users and problem reports, while the server daemon maintains several log files which can be reviewed or processed using additional tools.

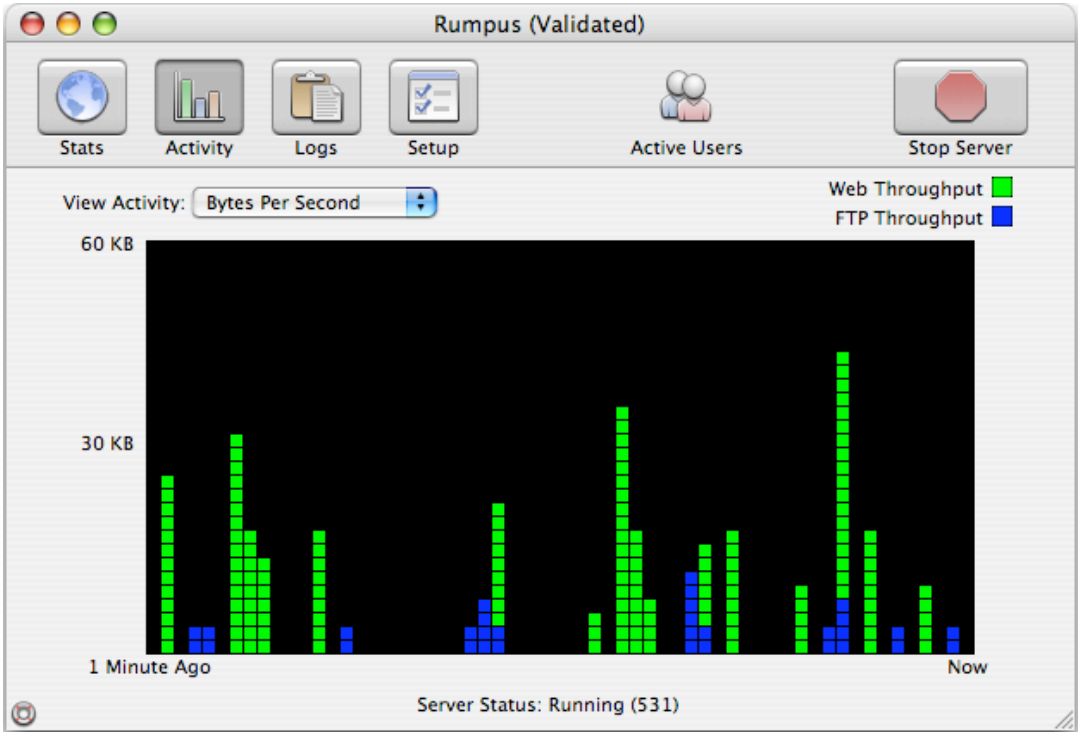
Monitoring Current Activity

The main Rumpus control window includes 2 different tabs that display information about recent activity. The Statistics ("Stats") tab, which is shown below, includes basic server statistics for both FTP and the Web File Manager.



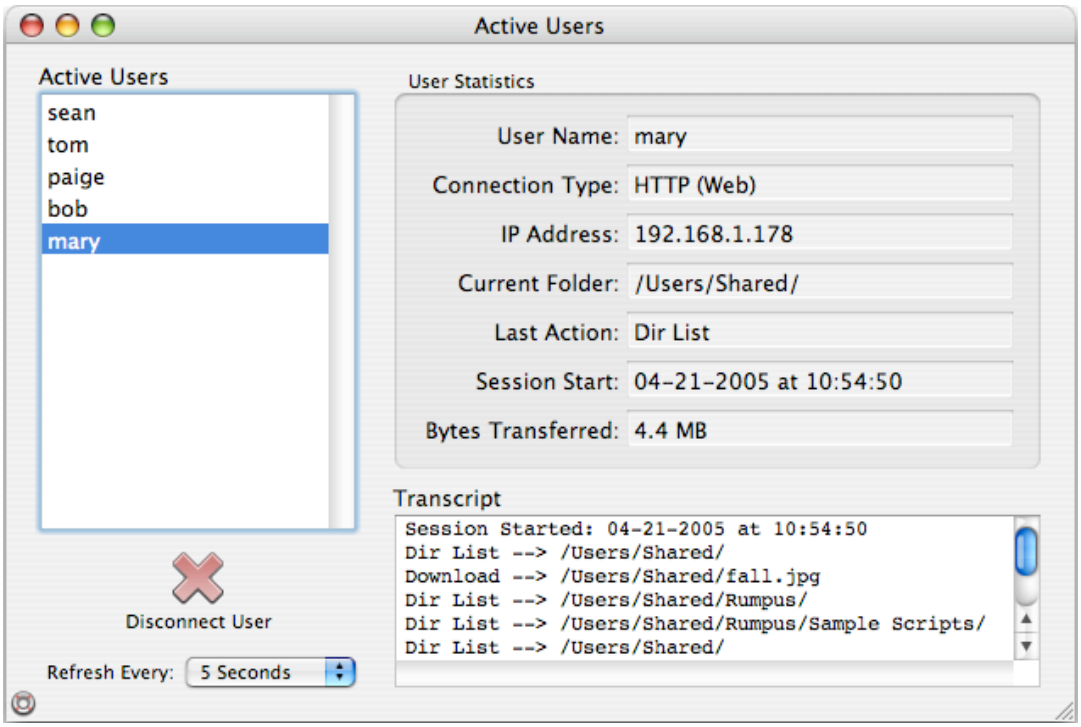
The display reflects activity since the last time the server was started. For details on the meaning of each statistic, open the "Server Status" help page in Rumpus by clicking the life preserver icon.

Server activity can also be displayed graphically, using the "Activity" tab of the main Rumpus control window. The graph, which also displays information only since the last time the server daemon was started, show server accesses or bytes transferred for both the Web File Manager and FTP over the past minute, hour, or several days.. Again, for full details on the data represented in the graph, see the help page in the Rumpus application by clicking the life preserver icon.



Active/Recent User Access Detail

While the server statistics and activity log tabs provide a high-level snapshot of server activity, a fine level of recent user access is also available. Click the "Active Users" button on the Rumpus control window for a list of users that have recently logged in to the server, and review their session activity. The Active Users window is shown below.



The Active Users list at the left of the window shows the user account name for each session that has been active within the last hour. Selecting the username in the list populates the User Statistics that relate general information about the session, as well as the session transcript, if transcripts are enabled. (To enable session transcript tracking, see the "Logs" tab of the FTP Settings window.)

Maintaining the information on the Active Users window requires a bit of extra overhead for the server, especially when it is under load and many users are accessing the system. When not actively reviewing user access, it is generally best to leave this window closed to avoid this overhead penalty. Keep in mind that user session information, and even session transcripts, are maintained by the server daemon process. This means that the Active Users window can be closed and re-opened at any time without loss of session information. In fact, the Rumpus control application can be quit for any length of time, and when re-launched, all server statistics will remain up to date.

Reviewing Recent Error And Debug Logs

Occasionally, you may have users that are unable to connect or upload files, or encounter other problems with the server. When this happens, a session transcript from the FTP client often provides the best indication of where the problem lies. Because the client initiates the FTP connection as well as each individual action, a transcript from the client may include details that aren't included in server-side logs. However, if the client is able to at least make a connection and send commands to the server, error can usually be detected by looking at the server error and debug logs.

On the main Rumpus control window, switch to the "Logs" tab. You can review each log file maintained by Rumpus by selecting the file from the "Viewing Log" pop-up menu. For problem troubleshooting, the Debug and Error logs will usually provide the best information. The Debug log includes the same errors that are reported in the Error log, plus a great deal of additional information, depending on the "Log Level" selected. The Debug log can become difficult to read, however, so the Error log is useful for filtering out everything but certain problems identified by the server.

Log Files

In addition to the Error and Debug log files maintained by Rumpus, several others are also available, each of which serves a different purpose. Each of the log files will be stored in the folder specified on the "Logging" tab of the FTP Settings window. For details on selecting the folder or enabling these logs, see the FTP Settings help page (or the WFM Settings help page, in the case of the Web Server log).

User Activity Log

Information recorded in the User Activity log includes IP address, the time and date of the connection, and the command issued by the user's FTP client, along with the result of each command.

Anonymous Password Log

Anonymous FTP users traditionally enter their e-mail address as their anonymous FTP password, so this log can be useful for the Rumpus administrator to determine who has been accessing the server without authenticating as a known secure user.

Failed Access Log

This log can be used to warn you about unauthorized users attempting to hack into your FTP server. It will also warn you about server problems or potential errors. For example, the log will show you if users are being rejected due to the maximum number of simultaneous users.

Web Server Log

A log file that includes a single line for each transaction processed by the Web server can be maintained. The log file will be stored in the defined log files folder (see the FTP Settings window) with the name "WFM.log".