# Server Setup

The Setup tab of the main Rumpus management window is simply a menu of additional server setup and management functions within Rumpus. For specific details on using these various functions, see the help page linked from the help icon (the life preserver in the lower-left corner) on each window.

## Install Server

The Rumpus application is actually made up of 2 distinct components: the control application and the server daemon. The control application is the graphical front end to controlling Rumpus, while the server daemon is the faceless Unix background process that actually provides FTP and Web services for incoming clients. The Installation window allows you to install, remove and update the daemon portion of Rumpus using the control application.

## FTP Settings

When first getting started running an FTP server, most people find that Rumpus works very well in it's default configuration. Over time, however, you may decide to alter certain aspects of your server's operation by adjusting the server-wide options that are available.

## Web Settings

The Rumpus built-in Web server provides HTTP (Web) services for two distinct reasons. First is remote user account administration, which allows you to manage user accounts from any Web browser. The second reason Rumpus includes a Web server is to allow users to transfer files with a Web browser via the Web File Manager. Both of these functions are controlled using the Web Settings window.

## Folder Sets

In most cases, assigning each user account a user folder and a set of access privileges is all that is needed to adequately restrict user access to the server. However, there may be times when you need to permit additional access to select folders, or add restrictions. For example, you may decide to create a "public access" folder, with access granted to several users (by dropping an alias to the public folder into each user's home folder) for downloading only. Or you may decide to restrict users to download-only access to most areas of your server, but create an "uploads" folder specifically for file uploads.

Overriding default user account privileges on a folder-by-folder basis is done using "Folder Sets". A Folder Set simply identifies one or more folders which

have specific permissions associated with them, and which can be assigned to a user account to provide expanded or restricted access to the folders in the set.

**Define Users**

The process of requiring that new users supply a username and password to gain access to a file server is called "authentication". To manage this process, Rumpus allows you to create and manage "user accounts", records that are associated with a username and include a variety of options that will serve to define the capabilities each person who accesses the server is given.

Put simply, Rumpus allows you to define user accounts which will be used to enforce access to your server based on a supplied username and password, and which will allow you to give different levels of access to different people. Think of user accounts as "preferences" that can be set individually for each person who will be logging on to your server.

**Upload Notices**

Upload Notices allow you to have an e-mail message sent when selected users upload new files to your FTP server. The Upload Notice window allows you to create any number of notices, each of which defines who should receive the e-mail and how it should be sent. As part of the user account setup (on the "Define Users" window), you can then select a notice to be used when each user uploads a new file.

**File Types**

For the most part, Rumpus handles file transfers without regard for the contents, or type of data, the file holds. There are a couple of instances, however, where it is beneficial for Rumpus to be able to recognize the type of file it is handling. It does this primarily based on the filename suffix, which is the portion of the filename following the period (or "dot"). Common suffixes include ".html", ".gif", ".doc", etc. Rumpus allows you to maintain a list of "File Types" which associate filename suffixes with file types for 2 important purposes.

First, when files are uploaded via FTP, the Mac OS "file type" and "creator" codes are lost (unless the file is uploaded using MacBinary encoding). File type and creator codes are what the Mac OS uses to display file icons in the Finder, determine what application to open the file in when it is double-clicked, etc. Under more recent versions of the Mac OS and OS X, filename extensions are also used for this purpose, but file type and creator codes are still supported and used as well. Using suffix mappings, Rumpus can correctly assign these codes to uploaded files, making working with them more convenient.

Rumpus suffix mappings are also used by the Web File Manager when files are

downloaded to a Web browser. The HTTP protocol allows a server to specify the data type for any file sent to the browser, and this information is used by the browser to correctly display or store the file. Rumpus sends the content type for each file served via the WFM based on the file's suffix.

### Block Clients

Over time, you may find unauthorized clients attempting to gain access to your server. This may be due to malicious people intentionally attacking your server or virus-infected computers randomly blasting any server they can find. In either case, the most efficient and secure way to handle such clients is to block their incoming connection requests as soon as they are detected.