# Allowing Users To Access Your Rumpus Server

An Overview Of User Account Setup For First-Time FTP Administrators

The basic operation of a file transfer server boils down to two key components: accepting connections over the network (including the Internet) and recognizing and managing each unique user. Providing the basic FTP service, and the networking required to support it, are covered in several other articles in this Rumpus package. Here, we'll focus on creating and maintaining the "user accounts" which will allow the server administrator to manage the various people who will transfer files to and from the server.

User Accounts

The FTP protocol requires that anyone who wishes to use the server log in, supplying a username and password, in order to begin a session. In Rumpus, you will create one or more "user accounts", each of which will have a unique username. It is easiest to think of a user account as the definition of a particular person who will be using your server, though a user account could also be created for a group of people, in which case each person in the group would use the same name and password. For now, we will assume that each person who will use your server will be given his or her own unique user account.

To create a user account (in other words, to give a new person access to your server), open the "Define Users" window in Rumpus.
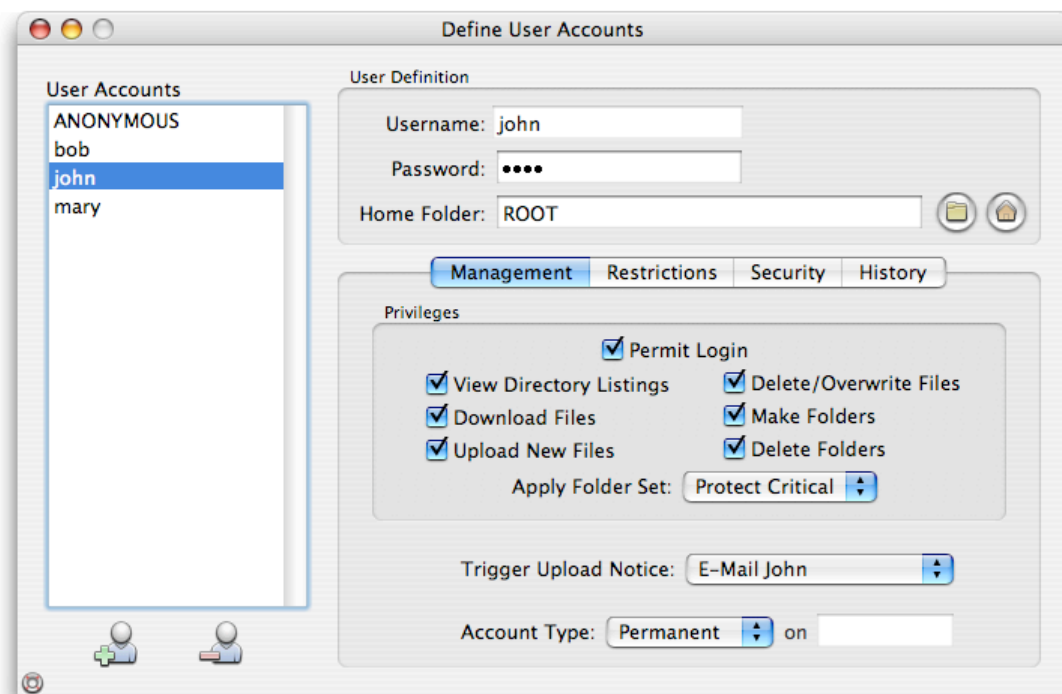
In the screen shot, three secure user accounts have been created ("ANONYMOUS" is a special account set aside for unsecured users, which we'll discuss later), and the account "john" is selected. Each of the fields on the window can be set independently for each user account, and will reflect the user account currently selected in the "User List". In this case, john's name and access privileges are displayed and can be edited.

The "Privileges" checkbox group defines the actions that the user can or can't perform. For a secured, fully activated user, all privileges should be enabled.

To create a user account, click the "Add New User" button just below the user list. A sheet will drop down asking you to supply the name and password of the new account. After completing the sheet, privileges and other account options can then be set. When you are done defining accounts, just close the window.

Common Settings

When you are creating your first few user accounts, most of the available account options can be left at their defaults, at least initially. There are a few options, however, you may need to consider right away:

Home Folders - *Giving Each User Their Own Space*

> In many cases, FTP users are completely unique, so that each has their own area on the server and is restricted from viewing other user's files. There are a couple of ways of accomplishing this, but the easiest and most reliable is to use "Home Folders".

> To start, create a folder on the local system for each user who will need their own space. We strongly recommend that these "user folders" be placed in the FTP Root folder, which is the folder "/Users/Shared/" by default. Name user folders so that they are easy to recognize and distinct for each user account. In fact, giving the folder the same name as the user account is a very good idea.

> Back in Rumpus, select the user account (or create a new one, as described above) and click the folder button next to the "Home Folder" field. In the standard Mac file/folder selection box that opens, select the user folder you just created. That's it... When a user logs in to your server with the defined name and password for that account, the view they will see of your FTP server will be limited to their own user folder.

> In most cases, the "Allow User To Move Out Of Home Folder" checkbox (found on the "Security" tab of the Define Users window) should be left off. This option tells Rumpus whether or not users should be able to move out of their own folder hierarchy. When the option is disabled, users will

not be able to see anything outside of the contents of their own folder (and it's sub-folders). If you turn the option on, users will initially be logged in to their own FTP user folder, but will be able to move up into the "FTP Files" folder and then back down into the folders of other users. In some cases, this is a handy feature, but when each user is unique and should be denied access outside of their own folder, "Allow User To Move Out Of Home Folder" should remain off.

Drop Boxes - *Blind File Uploads*

Another common use for FTP servers is the "Drop Box", in which case a user can upload files, but is not allowed to download or even see files that already exist on the server. Creating a drop box is as easy as setting the "Privilege" checkboxes correctly.

To define a drop box user account, create the account normally, including assigning a Home Folder as described above. Then enable the "Permit Login" and "Upload New Files" privileges, and leave all others off. In particular, with the "View Directory Listings" privilege disabled, users logging in with the given user account will not be able to see existing files already on the server.

The Anonymous User

Rumpus predefines one special user account: "ANONYMOUS". This is the guest account that all FTP clients and servers use for unsecured access. In other words, if you want to provide public, no-password-needed FTP access, enable the "Permit Login" privilege for the ANONYMOUS user account, and configure the other user account settings for this special user accordingly.

When FTP client applications log in without the user supplying a name and password, they will automatically send the name "Anonymous" and will normally send the user's e-mail address as the password. If you don't want to allow unsecured access at all, simply turn off the "Permit Login" privilege for the ANONYMOUS user account.

User Accounts And The Web File Manager

The Rumpus Web File Manager respects all FTP user account settings, so whether users connect via FTP or WFM, the same user setup options all apply. User home folders and drop boxes, for example, work equally well when a user logs in through a Web browser using the WFM versus via FTP. In fact, the same user can access the server one time through the Web File Manager and the next over FTP, and their view of the server will remain consistent.