

# Remote Administration

**Complete instructions for managing your Rumpus server from your desktop.**

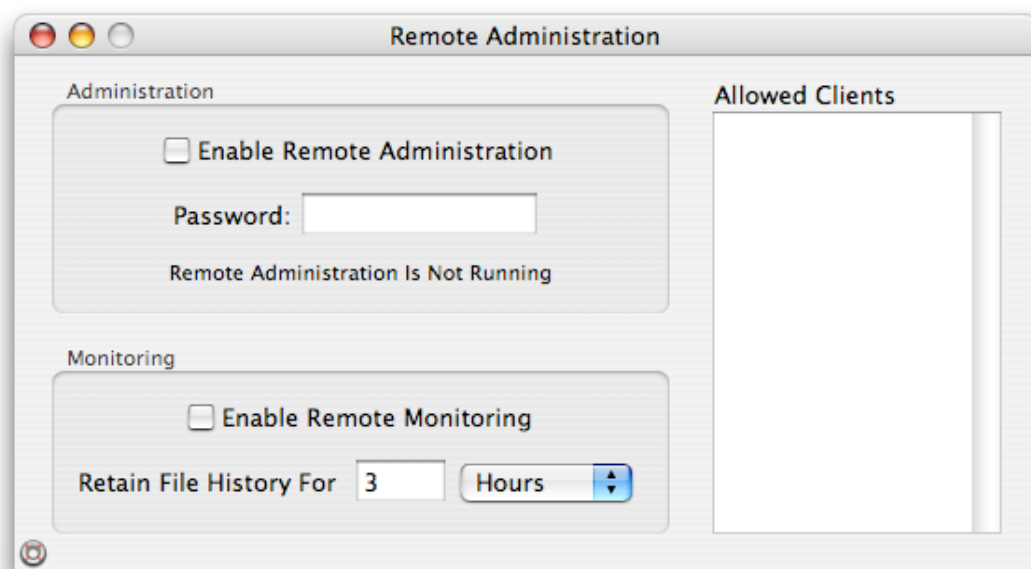
Rumpus allows you to add users, check server status, review logs, and generally administer your server from your own desktop Mac, rather than having to go to the server to perform these tasks. Setting up Rumpus for remote administration is fairly straightforward, though some effort needs to be expended making sure your Rumpus settings remain secure, even when you make them accessible to remote Macs.

## Before You Begin

Not all administrative tasks can be performed remotely. In particular, server installation, the setup assistants, and automatic diagnostics must be performed on the server itself. Almost all Rumpus control features needed for long-term server maintenance are accessible remotely, but before enabling remote access, you will need to install and perform basic setup of the server. In fact, we recommend that your server be functional and that you at least test the ability to log in to the server before attempting to remotely administer it.

## Preparing The Server

Once basic operation of the server has been established, you are ready to enable remote administration. On the “Management” tab in Rumpus, click the “Remote Admin” button. The remote administration control window will open, as shown below.



Maintaining security over remote administration is extremely important, so start by specifying an administration password and a list of client IP addresses that will be allowed to administer the server.

The remote administration password does not need to match any other password defined on the system or within Rumpus, and it will be used exclusively to control remote administration access via the Rumpus control application. Make sure the password you choose is suitably long and nontrivial, making it hard to guess. Be sure to remember the password, as it will be required to access the server from a remote Mac.

Next, specify one or more IP addresses from which you will use the control application to administer Rumpus. Partial IP addresses are allowed, such as “192.168.1.” to allow any client on the subnet “192.168.1.” to administer the server. Multiple addresses may be specified, one on each line of the list. Maxum very strongly recommends that this list be kept as short and as specific as possible. For example, if you plan to administer Rumpus only from your desktop Mac, then add only that computer’s full IP address. Do not specify unnecessary addresses, and do not specify entire subnets unless absolutely necessary.

With the security settings defined, check the “Enable Remote Administration” checkbox. This checkbox does not merely set a preference in Rumpus. When enabled, the remote administration daemon will be copied into your Rumpus daemon directory, a startup script will automatically be installed to launch the remote admin daemon at system start time, and the remote admin daemon will be started. Unchecking the box will stop the remote daemon, delete it, and delete the startup script.

A separate daemon is required to perform actions that the Rumpus server itself can’t, such as stopping and starting the server. The daemon is very small and will consume virtually no system resources.

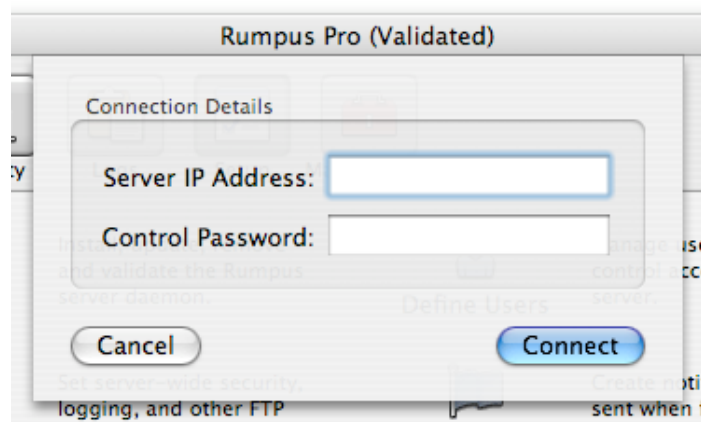
## **Firewall Considerations**

If the server has firewall software enabled, including the OS X built-in firewall, it will need to be modified to allow control connections. Incoming connections on ports 2998 and 2999 will need to be allowed, at least from permitted client IP addresses. (Two ports are required so that the control application can communicate with both the remote control daemon and the server daemon.) This process is essentially the same as creating holes in the firewall for FTP and WFM connections, so see the “Firewall Setup” article for detailed information on configuring the OS X firewall.

## **Remote Administration**

With the server set up to allow remote access, you are now ready to control it from another Mac. Place a copy of the Rumpus application on the desktop Mac you wish to use to control the server. Now, simply launch Rumpus, and when the setup assistant opens, close it by clicking the close box.

To establish a control connection, choose “Remote ...” from the “File” menu (Command-R). A sheet drops down allowing you to specify the server you wish to control, and your administration password.



After entering the server address and password, click Connect to initiate the connection. A dialog box will open, telling you that a connection was made, or if there was a problem, what the problem was. If this is the first time you have connected to the server, Rumpus will ask you if you would like to save the connection as the default setup for this computer. Once a default connection has been set, whenever you launch the Rumpus control application, it will immediately prompt you for the control password and connect. This makes it very convenient to set up your desktop Mac to routinely control your Rumpus server.

Notice that once connected, you can start and stop Rumpus service on the remote computer, review statistics , activity graphs, and log files, define users, and upload notices, manage server settings and edit file type and blocked clients lists.

## **Additional Notes**

The Rumpus remote administration function is designed primarily to allow one or more Rumpus control applications to control a single server. You can control multiple servers simply by entering the correct address when connecting, but Rumpus will not remember more than

one server address between sessions. It is also important to limit the number of clients simultaneously managing the Rumpus server, as it is possible for one remote connection to overwrite changes made by another, or by the control application running on the server itself. In general, it is best to have only one Rumpus control application open and managing your Rumpus server at any given time.

If you should ever need to install the Rumpus server daemon on a Mac that has been configured to control another server, open the “Install Server” window and click the “Remove Daemon” button, which will delete the Rumpus settings on that Mac. Next, quit and restart the Rumpus application. When the control application is launched without these settings, the setup assistant will open and guide you through a fresh installation of the Rumpus server.

One Rumpus server can be used to control another. At any time, you may choose “Remote ...” from the “File” menu to connect to a remote server, even when the Rumpus server daemon is installed on the client Mac. Once the connection has been established, all control functions will be performed on the remote server until you select “Disconnect” from the “File” menu, at which point control will resume over the local server settings.

Remote administration is performed using TCP/IP connections on ports 2998 and 2999. Commands issued by the Rumpus controller, and server responses, are not encrypted. Basic security precautions include IP address-based control restrictions and administrator passwords on each configuration management request. Maxum does not recommend that remote administration be used or enabled in environments where security is a primary concern.