# Remote Administration

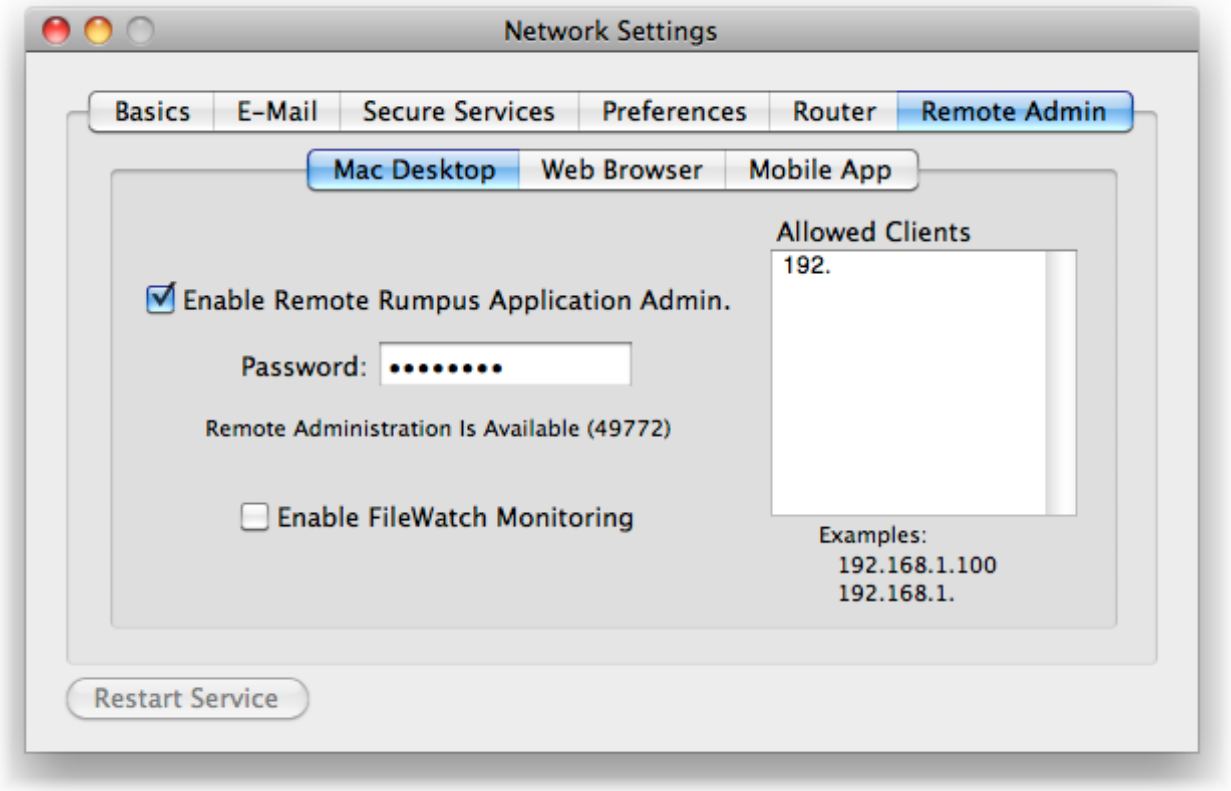
## Contents

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.

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. Open the "Network Settings" window and flip to the "Remote Admin" tab, shown below.




*Setup of remote administration from a desktop Mac*

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.

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. Keep the list 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.

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

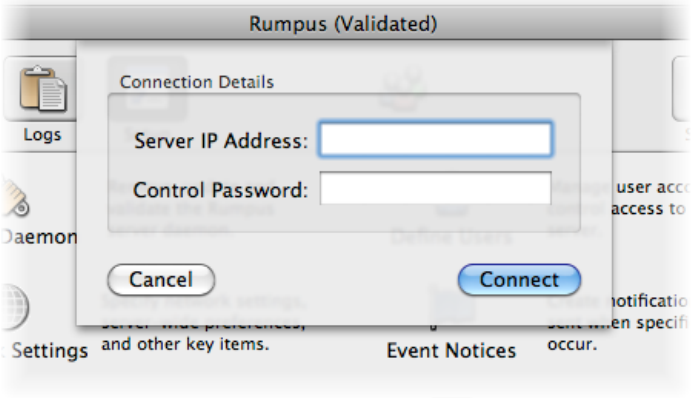
If the server has firewall software enabled, including the OS X built-in firewall, it will need to be modified to allow control connections. Incoming connections on ports 2998 and 2999 will need to be allowed, at least from permitted client IP addresses. (Two ports are required so that the control application 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.

# Performing 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.

**Important!** Do not install the Rumpus server daemon on Macs you wish to use to remotely control the server. If you have already installed the Rumpus service on the remote control Mac, open the "Server Daemon" window and use the "Remove Daemon" function to remove it. When the Rumpus control application is used on a Mac that does not have the Rumpus server daemon installed, remote control settings will be saved automatically, greatly simplifying the connection process in the future.

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.




*Making a remote control connection*

After entering the server address and password, click Connect to initiate the connection.

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.

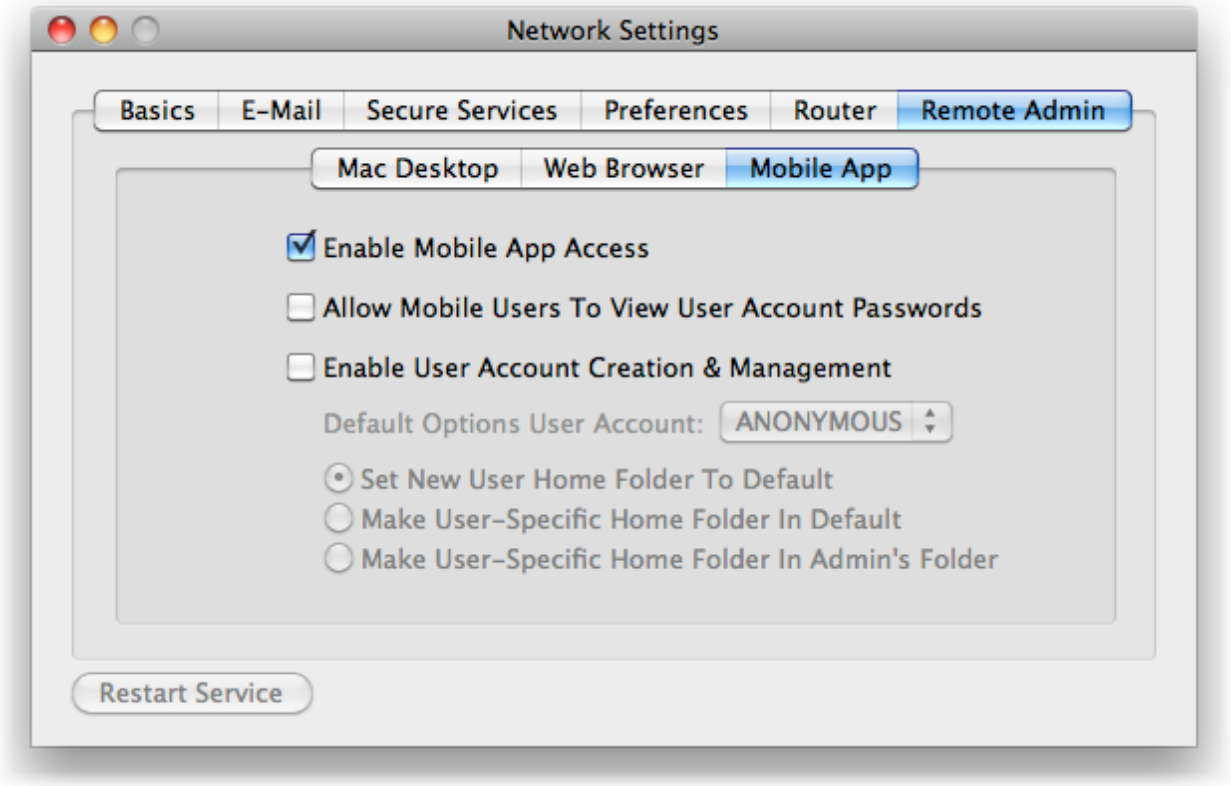
If you should ever need to install the Rumpus server daemon on a Mac that has been configured to control another server, open the "Server Daemon" window and click the "Remove Daemon" button, which will delete the Rumpus settings on that Mac. Next, quit and restart the Rumpus application. When the control 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.

# Mobile Application Administration

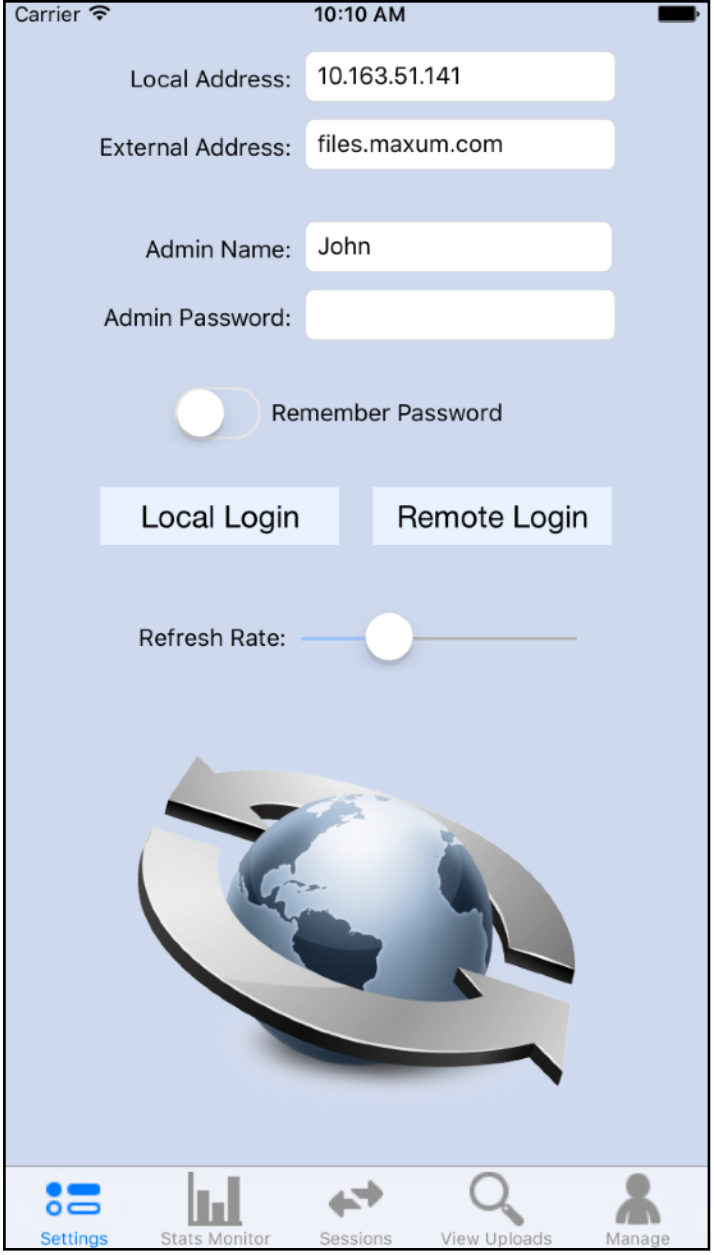
Basic server administration, including review of current user activity and recent file uploads, as well as simple user account management can be performed using the Rumpus iPhone app. To prepare the server to allow management from your iPhone, flip to the "Mobile App" tab on the Network Settings window.




*Enabling iPhone application administration*

Once mobile remote administration is enabled, download the Rumpus iPhone app from the iTunes app store, as you would any iPhone application.

The Rumpus app will need to know your Rumpus server's address and your administrative name and password, so before starting the Rumpus app, go to your iPhone settings and select the Rumpus app settings. Supply the server address and your administrative account name and password in the fields provided.


Carrier
10:10 AM
Local Address:
10.163.51.141
External Address:
files.maxum.com
Admin Name:
John
Admin Password:
Remember Password
Local Login
Remote Login
Refresh Rate:
Settings
Stats Monitor
Sessions
View Uploads
Manage

*Rumpus iPhone connection settings*

Most of the features of the Rumpus iPhone app are similar to features offered in the Rumpus application itself, optimized for the smaller mobile screen. There are 4 main tabs, selectable at the bottom of the screen, allowing you to choose among:

**Statistics** The Statistics tab is handy for viewing general server activity and confirming overall server operation.

**Sessions** This tab displays each active user session, including the user's current or most recent action and progress during the course of an active file transfer.

**Uploads** The Uploads tab lists files recently uploaded to the server. Tap on a file in the list for a reduced-size preview image of the file and additional transfer detail.

**Manage** Several basic server management functions are controlled on this tab.

For example, displayed below is the "Uploads" tab, first with the recent file uploads list shown, and then the result of tapping on the "Darts.jpg" file in the list.


*The Rumpus app "Uploads" tab*

## Managing Users In The iPhone App

A simplified form of user account management is provided in the iPhone app. To streamline the user account management interface, most user account options have been removed and the system assumes that all iPhone-created users accounts should be assigned a well-defined Home Folder.

Account administration is enabled on the "Mobile App" tab of the Network Settings window, but the first task is to define a user account which will be used as a template for all account settings for new accounts. Open the Define Users window and create a new user account named "iPhoneTemplate", or something similar. Set the password to a long string of random numbers and letters, so that the account won't accidentally be used directly. Finally, set all account options to the values you would like applied to new user accounts created via the mobile app.

On the Network Settings window, select the iPhone template user account from the "Default Options User Account" pop-up menu. Finally, choose one of the following 3 options for assigning new user account home folders:

### Set New User Home Folder To Default

With this option selected, new users will be assigned the home folder set in the iPhone template account. For example, if the home folder specified in the template account is "/Users/Shared/Guests/", then that folder will be assigned to new user accounts as well.

### Make User-Specific Home Folder in Default

In this case, when a new user account is created, a new folder will be created and assigned as the home folder. This new folder will have then name of the user account itself, and be located in the home folder defined in the template account. For example, if the home folder specified in the template account is "/Users/Shared/Guests/", and a new user account named "Paige" is created, the new account home folder will be "/Users/Shared/Guests/Paige/".

### Make User-Specific Home Folder In Admin's Folder

With this option, when a new user account is created, a new folder will be created and assigned as the home folder. This new folder will have then name of the user account itself, and be located in administrator's own home folder. For example, if the administrator "Tom", whose own home folder is "/Users/Shared/Admin-Tom/", creates a new user account named "Sean", the new account home folder will be "/Users/Shared/Admin-Tom/Sean/".

When a new user account is created in the iPhone app, only the account username, password and basic access privileges can be assigned by the administrator. All other account options will be automatically set to those defined in the template account.