

Firewall Setup

Configuring the Mac OS X firewall to allow FTP and WFM connections.

Getting Started

The basic job of the OS X firewall is to block unwanted network access to your computer, so when your firewall is enabled, it will need to be configured to allow external users to connect to Rumpus FTP and Web services. When you are just getting started with Rumpus, it is usually best to temporarily disable the firewall, eliminating the possibility that it will interfere with service. Once you have confirmed that your Rumpus server is running and available, the firewall can be re-enabled and setup as needed.

To disable the OS X firewall, open the System Preferences window and select the “Security” panel, then switch to the “Firewall” tab and choose the “Allow all incoming connections” option. FTP and Web services should now be accessible to other computers on your LAN, and the Internet in general when your network is configured properly.

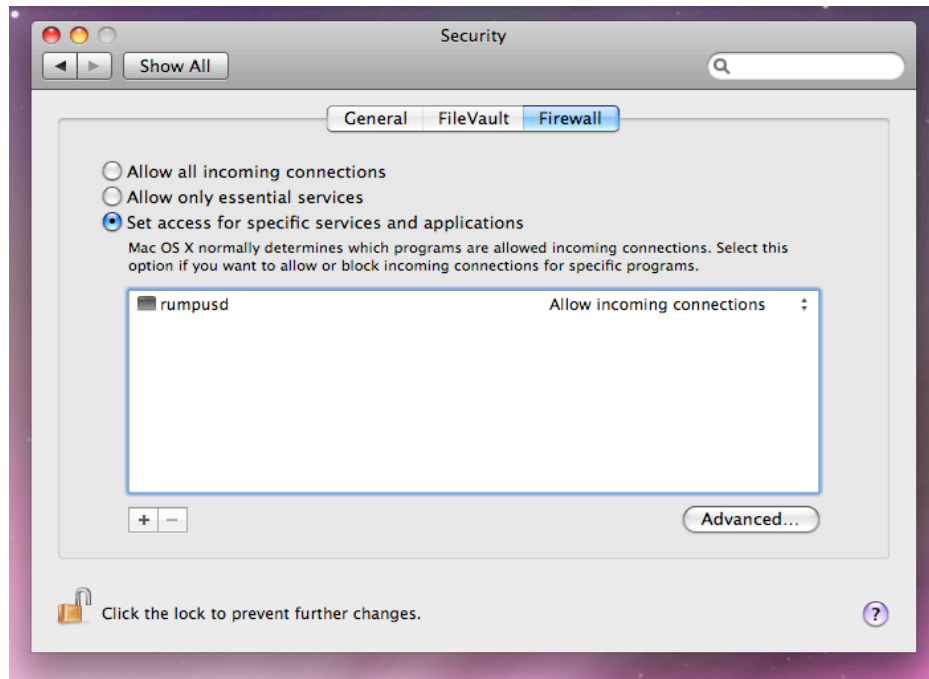
Configuring The Firewall

Rumpus can be run indefinitely with the firewall off, but for better server security it is usually a good idea to use the firewall to restrict access to explicitly allowed services. To enable the firewall, choose “Set access for specific services and applications” on the “Firewall” tab of the Security System Preferences panel.

To enable incoming connections to Rumpus, you will need to allow inbound connections to the Rumpus server daemon. To begin, click the “Open Config Folder” button on the “FTP Settings” window in Rumpus. This will open the Rumpus configuration folder, which is normally hidden in the Finder and contains the Rumpus daemon application.

Next, on the “Firewall” tab of the Security System Preferences panel, click the “Add” button to add an accessible service. When the standard file selection sheet drops down, drag the “rumpusd” application from the Rumpus configuration folder into the file listing on the sheet. This will cause the “rumpusd” file to be selected automatically, and you can then complete the sheet.

Make sure that the rumpusd application is added to the list of accessible services, and is set to “Allow incoming connections”, as shown below:



With the firewall on and the “rumpusd” entry created, you should now be able to access your Rumpus server while the OS X firewall blocks access to all other restricted ports. If you have trouble connecting to the server from another computer on your LAN after completing this procedure, be sure to contact Maxum Technical Support at “support@maxum.com”.

Remote Rumpus Administration And SSL Encrypted Sessions

Two other daemons may also be run as part of a Rumpus server, depending on your configuration. The first is the “Rumpus Remote Daemon”, which allows the Rumpus application to be run from remote Macs, if necessary. The other is Stunnel, which provides SSL tunneling for both HTTPS and FTPS services. These daemons will also need to be added to the list of applications that are allowed to accept incoming connections, if you decide to make use of these services.

The Rumpus remote daemon is called “rumpusremoted” and resides in the same Rumpus configuration folder as the main rumpusd daemon. It can be added to the list of applications allowed to receive connections in exactly the same way the rumpusd daemon was added.

The Stunnel daemon is called “stunnel”, and it resides in the Stunnel configuration folder. Open the “SSL Setup” window and click the “Open Stunnel Config Folder” button on the “Options” tab to open this folder in the Finder, then add the stunnel daemon to the allowed list as described above.