# Rumpus Overview

## Contents

# Welcome

Welcome to Rumpus!

At its core, Rumpus is a very complicated piece of software.  In a single product, Rumpus combines FTP, WebDAV, HTTP, SFTP, FTPS and HTTPS services.  As the server administrator, you will manage Rumpus as a single file sharing platform, but in reality, each of these are unique server engines built into one program.  On top of that, Rumpus supports mail notifications, scripted extensions, a variety of security functions, multiple user authentication mechanisms, the ability to create and process Web forms, and dozens of other features.

As with any complex and flexible software, setting up and administering a Rumpus server is not trivial.  However, we have worked hard to make Rumpus powerful, stable, and as easy to use as possible.  We think you'll find that most setup and administrative tasks are logical and intuitive, but if you have any trouble, please send e-mail to "support@maxum.com" and give us a chance to help.

# Quick Start

Rumpus is, quite simply, the easiest way to run your own file transfer server.  After completing the short Setup Assistant, your PC will be ready to act as a fully functional FTP server, and Web browsers will also be able to connect and transfer files.

## Getting Started

### *Step 1 - Install The Server*

The first time Rumpus is launched, the Setup Assistant will automatically open.  Brief instructions are provided at each step, and when you complete the assistant, Rumpus will provide details on connecting to your server from an FTP client and/or Web browser.

### *Step 2 - Try It*

From another computer on the local network, follow the connection instructions to test the server.  If you need to see the connection instructions again, click “Get Connected”.  Try a few sample file uploads and downloads to familiarize yourself with the basic Rumpus service.

### *Step 3 - Customize The Web Interface*

Customizing the Rumpus Web interface is a good way to explore Rumpus' flexibility. Open the "Web Settings" window in Rumpus to access the Web interface options. Try selecting different colors, enabling additional features or replacing the Rumpus logo with your own. Log into the server using a standard Web browser to quickly see the effect of your changes.

### *Step 4 - Set Your Network Options*

Other basic setup options are included on the "Settings" window. While basic operation of the server is possible within your LAN with almost no special configuration, setting your network options, mail server information, and other key settings on the Network Settings window is recommended when you are ready to fully deploy the server.

### *Step 5 - Configure Your Router*

If your Rumpus server is on a private network, linked to the Internet via router with a single network connection and IP address, be sure to review the  the information on the "From Outside Your LAN" tab of the "Get Connected" window. Configuring your network to allow outside users to connect is often the most difficult task when setting up a new server. The "Get Connected" information displayed by Rumpus will help, and a link to additional resources on the Maxum Web site is provided.

## If You Need Help

A number of very helpful articles are provided to assist you in getting started. These articles can all be found in the "Helpful Info" folder of the Rumpus package.

Maxum also maintains a set of frequently asked questions, and their answers. Visit our Web site at www.maxum.com for FAQs, late-breaking information and product updates.

You can also send technical questions to us via e-mail addressed to "support@maxum.com". We understand that support via e-mail can be a hit-or-miss proposition when dealing with some companies, but this is not the case with Maxum. E-mail is, by far, the quickest and most reliable way to get answers to your Rumpus questions.

### Standard Or Pro?

To meet the needs of smaller sites as well as large installations and ISPs, Rumpus is offered in both Standard and Pro versions. The Standard version supports up to 32 simultaneous users and 32 user accounts defined in Rumpus' built-in security. For larger sites and ISPs, Rumpus Pro supports up to 256 simultaneous connections, with no set limit on the number of accounts that can be defined. Rumpus Standard lacks the LDAP support of Rumpus Pro (because directory service authentication allows for an unlimited number of users), but in all other ways, Rumpus Standard and Pro are identical.

### Removing Rumpus

To remove Rumpus from a server, click “Stop Server” then quit the Rumpus application. Next, run the uninstall tool at "C:\Rumpus\unins000.exe". Finally, to completely remove your Rumpus settings files, delete the folder at "C:\Rumpus\".

## Upgrading

Maintaining a recent backup of your Rumpus settings is always a good idea, and is particularly important when performing major updates to the server. Rumpus updates are designed to preserve your setup, but backing up the server is the best way to ensure against data loss. To back up all Rumpus configuration, archive the folder "C:\Rumpus\Config\" to a safe backup location.

To upgrade Rumpus, simply launch the installer for that version and follow the installation prompts. User accounts and other settings will be brought forward to as great a degree as possible. Of course, in newer versions of Rumpus, administration options are often added or changed, so be sure to review your basic settings and test user access after the update is complete.

### If You Have Updated The WFM Templates...

As new features and improved functionality are implemented in Rumpus, changes to the WFM template files are necessary. For those who have customized the templates, this creates a problem when upgrading, requiring that you merge your changes into the new WFM template set.

**Important:** “Customizing the WFM template files” refers only to changes to the HTML/CSS files used to present the Rumpus Web interface. If you have customized the interface by altering colors, fonts, the logo file and other options within the Rumpus application, those changes will be preserved automatically.

When upgrading, make sure you have a good backup copy of your customized WFM template files, then complete the Rumpus upgrade normally.  The latest WFM templates will be installed, overwriting your customized files.  When the update is complete, test basic functionality to ensure the server is working as expected.  Finally, re-implement any needed customizations in the new template set.

## Administration

There are two different interfaces for managing a Rumpus server: Web administration and the control application.

Most administration tasks can be performed either within the control application right on the server, or remotely using the Web administration function ("Server Setup").  This includes basic server settings, managing user accounts, creating and assigning Event Notices, and more.

A couple of administration functions, most notably setup of Upload Center forms, are available via Web administration only. And the Web Appearance settings, because the administrative interface is complex in places, are selectable only within the control application.

## Port 80 Conflicts: Disabling IIS

On some Windows installations, IIS is enabled by default.  This leaves you with two options: run Rumpus on an alternate port or disable IIS.  Running Rumpus on an alternate port is easy, just enter the alternate port number on the Web Settings window, Options tab.  But unless you are running IIS for a specific purpose on the same server, it's usually best to disable it so that Rumpus can be run on the default Web (HTTP) port, 80.

In Windows 10, open Settings and go to the "Administrative Tools" panel.  Next, open "Services", and then the "World Wide Web Publishing" properties panel.  To prevent IIS from being automatically started each time the system boots, set the "Startup Type" to "Manual".  Then either restart the server or click "Stop" in the "Service" area to stop the currently running instance of the built-in Web server.

With the built in IIS service disabled, Rumpus can then bind to port 80 and provide Web service on the server.

## Reporting Crashes

All non-trivial software has bugs, and Rumpus is no exception. Most people experience exceptional stability with their Rumpus server, but crashes do occur. We are committed to correcting problems, especially crashing bugs, in a timely manner when they are reported. Should you experience a crash, and we certainly hope that you do not, please report it so we can correct it.

When reporting a crash, please describe the circumstances under which it occurred. Sometimes, you may not know what caused a crash, but if you do, please provide as much information about what was happening at the time of the crash as possible.

Please also always include the Windows crash report. Crash reports can be found in the folder:

```
C:\Rumpus\Logs\
```

Crash report files will be named "rumpus.exe.1234.dmp", where the number "1234" will be any number. Please always send the most recent 2 or 3 reports. Sending 2 or 3 reports allows us to confirm that the cause of all crashes is the same, but there is no need to send more than that, even if they exist.

## Using Network Shares

User Home Folders, or even the entire Rumpus content folder (your "FTP Root" folder) can be located on network share points. Rumpus will treat network shares no differently than local storage space, and will allow users to upload, download and manage files on locally mounted network volumes with ease.

However, in order for the Rumpus daemon to be able to do this, the network share must be persistent mapped as the SYSTEM user on the Rumpus Server. The steps to perform this type of mapping are slightly different than a regular drive mapping:

1. Download PsExec from Microsoft and install on your Rumpus Server.
   https://technet.microsoft.com/en-us/sysinternals/bb897553
2. Open an elevated command prompt. (Run as Administrator.)
3. Make sure psexec.exe is in your path, or move into the psexec directory.
4. Become the SYSTEM user by issuing the psexec command:
   ```
   psexec -s cmd.exe
   ```
5. Create the persistent mapped drive as the SYSTEM user:
   ```
   net use z: \\servername\share /persistent:yes
   ```

To remove the drive mapping, follow steps 2-4, then run the command: net use z: /delete

NOTE: The drive letter z: is used as an example. You may use any drive letter available on your server.

# Frequently Asked Questions

## Rumpus launches fine, but users can’t connect.  What should I do?

By far the most common problem administrators have when getting started with Rumpus is not with Rumpus at all, but in setting up their network to accept connections from outside clients.  This requires configuring your router and working with your ISP to ensure external clients get properly routed to your server.  While this setup isn’t technically part of Rumpus administration, we have developed a number of helpful resources to clarify what needs to be done.

First, open the "Get Connected" window by clicking the "Get Connected" button on the main Rumpus Administration window.  Follow the instructions presented there to test connections via Web browser and/or FTP client running on another computer on the same local network.  Once you have confirmed local access (using the local address of the server), you can move on to getting external users connected.

On the Get Connected window, flip to the "From Outside Your LAN" tab.  The information there explains at a high level how your network needs to be configured based on your current Rumpus settings.  Maxum also maintains a “Get Connected” page on our Web site, which includes a dynamic troubleshooting guide to help you identify and resolve problems, along with additional details about how external users are routed to your Rumpus server.

http://www.maxum.com/GetConnected/

In addition, FTP and the networking needed to support it is described in fairly technical terms in the “FTP Technical Overview” article in the Helpful Info folder of this package.  System administrators interested in the details of how FTP works will find this article very helpful.

Please review these resources for help in diagnosing any “failed connection” problems.  Of course, if trouble persists, contact Maxum Technical Support at “support@maxum.com”.

## Most Web browsers work fine and can connect without trouble to the Rumpus WFM, but a few of my clients can’t make a connection at all.  What can I do?

The most common reason why some clients can’t connect to the WFM when most can is that the client is behind a firewall that is blocking the connection.  The usual reason for this is that Rumpus has been assigned a non-standard Web server port, and the firewall only allows clients to access Web servers on the standard port of 80.  If you are not running another Web server on the Rumpus computer, or on the same external Internet address used to connect to Rumpus, we strongly recommend that you choose port 80 for the Rumpus Web server port.  Be sure to have your router/firewall configured to allow and forward the correct port to the Rumpus server, whether it is 80, 8000, or some other value.

### My Rumpus server is configured to allow both FTP and Web (WFM) access. Some Web browsers, however, won't display the WFM interface, and instead either fail to connect or look really bad. What is the problem?

Does your server name begin with "ftp."?

The World Wide Web is based on the HTTP protocol. While many people refer to their Rumpus server as their "FTP" server, FTP is actually an entirely different protocol. Rumpus includes both HTTP and FTP services, built in. This is very convenient for you as an administrator, because Rumpus implements both protocols seamlessly, but it can create confusion when making connections.

Web browsers, by default, connect using HTTP, but some also are capable of using FTP. When these browsers connect to a server with a name that begins "ftp.", they will often connect via the FTP protocol instead of HTTP. FTP sessions don't provide the rich user interface offered by HTTP, creating a problem for the end user.

Have clients connect using the full URL of your server, including the leading "http://". This signals the browser to connect via HTTP, even though the domain name of the server begins "ftp."

To allow clients to consistently connect without the leading "http://", select a domain name that begins with something other than "ftp." For example, "files.acme.com" or "transfer.acme.com" will be more reliable than "ftp.acme.com", and avoid this problem completely.

### At seemingly random times, some users lose the ability to log into their user account. I checked the Define Users window, and discovered that the "Permit Login" privilege is disabled for the affected user accounts. What happened?

Rumpus includes a feature which will deactivate user accounts when users appear to be guessing to determine their password. If numerous incorrect password entries are received for the same account without a successful login, Rumpus disables the user account by removing the "Permit Login" privilege. The intention is to keep would-be hackers from setting up automated robots that repeatedly guess at user passwords to gain access to the server. To disable this feature, uncheck the "Disable User Accounts After Several Failed Login Attempts" option on the "FTP Settings" server settings panel.

### Most users can connect to my Rumpus server, but a few can’t. The user account looks OK, and I can even log in to their account from my computer. What should I check next?

In addition to the “Disable User Accounts After Several Failed Login Attempts” feature mentioned above, Rumpus also includes “Automatic Hack Attempt Recognition”. This feature watches for numerous incorrect login attempts from the same client computer within a short period of time, and automatically adds the client IP address to the “Blocked List” when this occurs. Open the “Blocked Clients” server settings panel, and remove the addresses of known users if they appear. To disable the “Hack Attempt Recognition” feature, or to make it less sensitive, see the related options in the “Security” section of the FTP Settings server settings panel.

### I can't seem to get e-mail Event Notices working. Any suggestions?

When setting up mail service in Rumpus, be sure to start with the Network Settings server settings panel. Once you have set the mail settings there, new e-mail Event Notices will default correctly based on that configuration.

In the "E-Mail" section of the Network Settings panel, use the "Send A Test E-Mail" function for relevant diagnostic information. The test function not only attempts to send the e-mail message, but checks for numerous common problems, and will include details on resolving the problem when possible.

### I am moving my Rumpus server to another PC. How can I preserve my user accounts and other settings?

All Rumpus configuration files are stored in the directory "C:\Rumpus\Config\", and can be copied normally for backup purposes, or to move settings from one machine to another. The "Rumpus.users" file is usually the most important, as it contains all of the user account definitions.

These files can be moved from one PC to another, but there are a couple of things to watch out for. The biggest issue is that the FTP Root folder and user Home Folder paths may change when moving the server to another machine, though other differences between the old and new computers may cause problems as well.

When moving your server (or re-installing after a system cleaning), we recommend that you start by downloading the latest version of Rumpus from the Maxum Web site. Next, run the installer and complete the setup assistant as if you were installing a brand new server. After completing the setup assistant, start the server and log in from another computer on the network, to confirm the installation.

**Important Note:** Do not attempt to simply move the entire "C:\Rumpus\" folder from one PC to another. The first step in moving a server is to install a fresh, up-to-date Rumpus service on the new server, then verify the default installation by starting the service and logging in from another computer on the same network. Be sure to perform this default install and connection test before attempting to move configuration files from the old server.

With the new server functional, stop the server and copy the "Rumpus.users", "Rumpus.notices", and other required files to the "C:\Rumpus\Config\" directory. It is usually best to copy only the files you need, to minimize the chance of conflicting with server-specific settings. Be sure to check your user accounts, especially the "Home Folder" paths, to make sure the account settings make sense on the new server.

With the necessary files replaced, start the server, and log in to at least a couple of user accounts to make sure the server is functioning perfectly.