



Rumplet: Desktop Drop Ship

Contents

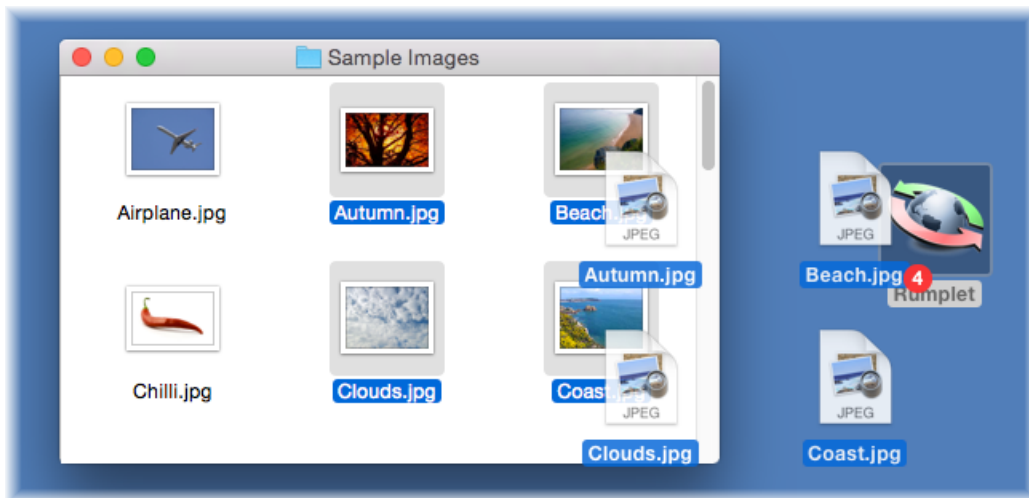
Drop Shipping Files	2
Reviewing And Managing Past Shipments	3
Configuring Rumplet For Access	4
Configuring The Server (Mac Servers)	6
Configuring The Server (Windows Servers)	6
Troubleshooting	7

Drop Shipping Files

Rumplet is a small, lightweight desktop applet that makes drop shipping files through your Rumpus server quick and easy.

Rumplet is not run on the Rumpus server, but rather on any client computer from which users need to be able to send large files to outside guests.

Once basic configuration options have been set (see the “Configuration” sections below for details), just drag any file, folder or even group of files that you would like to send onto the Rumplet application.



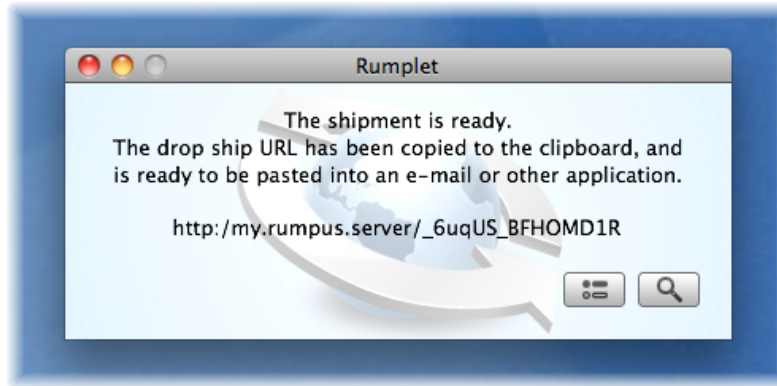
To send one file, several files, or entire folders, just drag them onto the Rumplet application.

If Rumplet is already running, files and folder can also be dragged onto the display window.



Or, drag files and folders directly into the Rumplet application window.

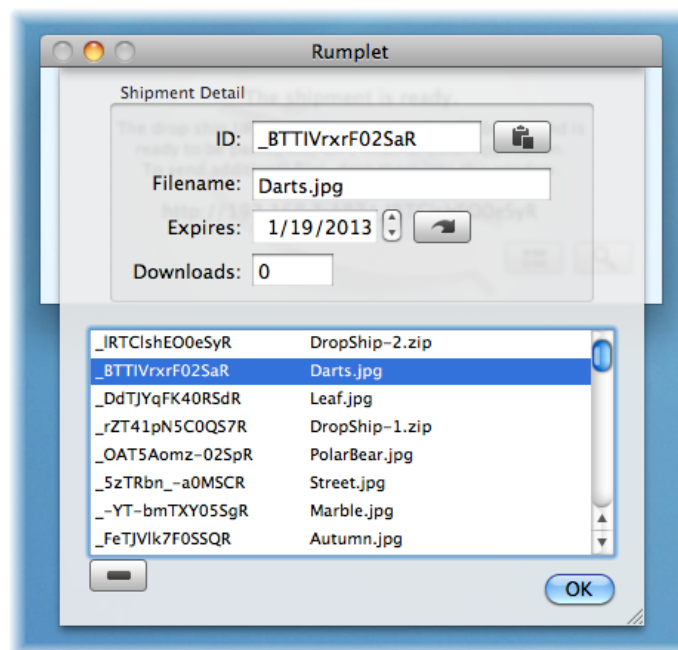
If you drag a folder, or multiple files or folders, into Rumplet, the entire package will be automatically zip compressed into a single archive file for easy downloading by your recipient(s). Individual files dragged into Rumplet will be sent without compression. In either case, the file will then be uploaded automatically to the Rumpus server, and a unique pickup URL will be generated and copied into the clipboard.



The drop shipment is now ready. Switch to your e-mail (or any other) application and paste in the drop ship URL.

Reviewing And Managing Past Shipments

To view drop shipments that you have already sent, click the "view" (magnifying glass) icon.



The "view existing drop shipments" sheet.

Past drop shipments are displayed in the list, with the most recent shipments shown at the top of the list. Additional detail is displayed for the selected shipment.

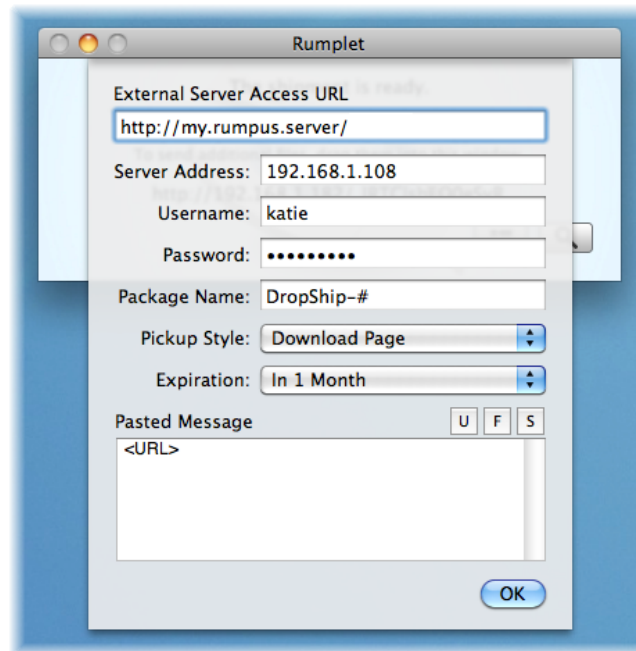
To delete a past drop shipment, select it in the list and click the remove button, just below the list.

Click the clipboard button to copy the drop ship URL for the selected shipment to the clipboard, for pasting into an e-mail (or other) application.

To change the expiration date of an existing shipment, select it, set the date to the desired expiration date, and click the reset button.

Configuring Rumplet For Access

When Rumplet is first run, the setup sheet will automatically open. In later Rumplet sessions, access the sheet by clicking the preferences button on the main Rumplet display window.



External Server Access URL

File pickup URLs are generated by Rumplet by combining the “External Server Access URL” and the drop shipment ID. If your server has been configured to support SSL encrypted Web service, the URL may begin “https://”, while standard Web pickup is identified by a URL that begins “http://”. The URL will normally include the public access IP address or server domain name of your Rumpus server.

Server Address, Username and Password

Supply the address of your Rumpus server, and the user name and password of the drop ship sender's Rumpus user account. When both the Rumpus server and the Rumplet client are on the same local network, be sure to supply the local IP address of the server, not the external address or domain name, for best performance.

Package Name

When a single file or folder is sent using Rumplet, the file or folder name is used to identify the file when delivered. However, when multiple items are moved at once, Rumpus generates a name for the complete drop ship package. The "Package Name" field allow you to customize the filename applied to multi-item shipments. The pound sign ("#") is used to denote a sequential number Rumplet will automatically maintain as packages are sent through the system.

Pickup Style and Expiration

The "Pickup Style" and "Expiration" options are identical to those options used in the Web interface drop ship function, as selected on the "Web Settings" window on the Rumpus server.

Pasted Message

When a shipment is sent, the drop ship URL is automatically copied to the clipboard for easy pasting into an e-mail or other application. If you wish, you may specify a more complete message to be copied to the clipboard.

The message may include the drop ship URL, the file name, and the file size, inserted into the message using the tokens "<URL>", "<FILENAME>" and "<FILESIZE>" respectively. To help avoid errors in tokens, use the "U", "F" and "S" buttons to insert the tokens at the current cursor position when the pasted message text field is active.

For example, a pasted message might look like this:

```
The file "<FILENAME>" (size, <FILESIZE>) is ready for pickup.
Click the URL below to download the file.
```

```
<URL>
```

```
Please contact Acme Widgets if you have any problems accessing
this file. Thank you!
```

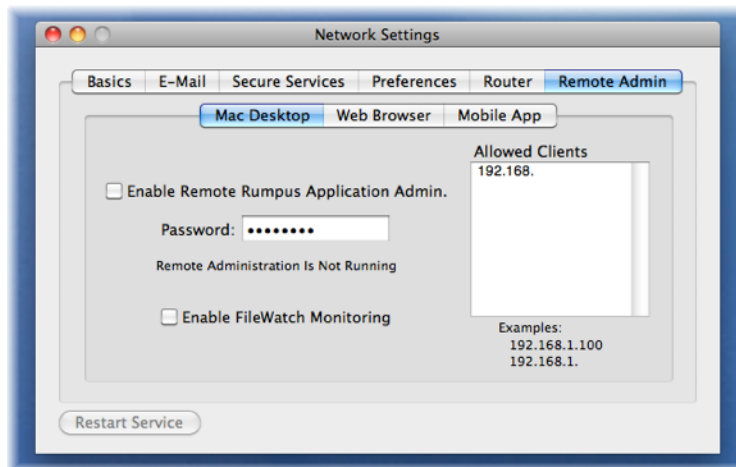
When a file is drop shipped, that message, with the URL, filename and file size inserted in place of the tokens, will be copied to the clipboard, ready to be pasted into an e-mail message body.

If you prefer to have only the drop ship URL pasted to the clipboard, set the pasted message to the token “<URL>”, with nothing more in the message.

Configuring The Server (Mac Servers)

In order to allow clients to drop ship files using Rumplet, some server configuration is required.

First, like all remote Rumpus server access, the IP addresses of Rumplet clients need to be supplied on the “Remote Admin” tab of the Network Settings window. In many cases, the most practical option is to allow all clients on the local network to drop ship files by supplying the subnet range in the “Allowed Clients” list, as shown below.



Rumplet users also need valid user accounts on the Rumpus server, with both the “Permit Login” and “Drop Ship Files” privileges enabled. To assign the needed privileges, open the Define Users window, select the account of the drop ship user, and check the boxes in the “Privileges” section.

Finally, note that communication between the Rumplet client and the server will be carried out over TCP port 2999. If there is a firewall running on the server, or any network device between the client and server that may restrict connections to the server, access on that port will need to be allowed.

Configuring The Server (Windows Servers)

On a Windows server, Rumplet access is enabled automatically, as long as Drop Shipping has been enabled and the user account configured in Rumplet has the “Drop Ship Files” privilege enabled.

Troubleshooting

If you have problems getting Rumplet clients connected to the server, here are some suggestions for getting back on track.

Check The Errors Log

When a Rumplet client gets a connection error, the first thing to do is check the error log in Rumpus (on the "Logs" tab of the main control window, select the "Errors" log). Try a test shipment or just open the "view past shipments" sheet from the Rumplet client, then on the Rumpus logs tab, click the refresh button. If the client was able to connect, but the Rumplet request was refused by the server, a log entry should explain why. If no entry is displayed in the log, it's likely that a network connection from the client to the server can't be made, possibly for one of the reasons described below.

Make Sure The Client IP Address Is Allowed (Mac Servers Only)

In Rumpus, open the "Network Settings" window and flip to the "Remote Admin -> Mac Desktop" tab. Make sure that the IP address, or subnet, of the client is listed in the "Allowed Clients" list and that "Enable FileWatch Monitoring" (required for Rumplet access) is turned on. The "Allowed Clients" list uses a "begins with" check of client IP addresses, so an entry of "192." will allow any Rumplet client whose IP address begins "192.". If you want to allow Rumplet access from any IP address, anywhere on the Internet, enter the numbers 1 through 9, one number on each line, in the list. This will cause Rumpus to allow Rumplet users from IP addresses that begin with "1", "2", "3" and so on, in other words, all addresses.

Make Sure The Server Is Accessible On Port 2999

If you are running a firewall on the server, make sure the firewall is set to allow access on port 2999. If connections are going through a port forwarding router (as is the case when the server is on a private network and you want to allow outside users to run Rumplet), make sure port 2999 is set up for forwarding.

Check Your Rumplet Setup

Open the Rumplet setup sheet and confirm that each configuration field has been set correctly. The "Server Address" should be set to an IP address or domain name only, and the address should be the most expedient address possible. For example, on a private local network, you should supply the LAN address of the server, rather than the external address or domain name, with no "http://" or other extraneous protocol specifications. By contrast, the "External Server Access URL" must be a full URL that begins either "http://" or "https://". Put simply, this is the full URL external users enter in order to access your server.