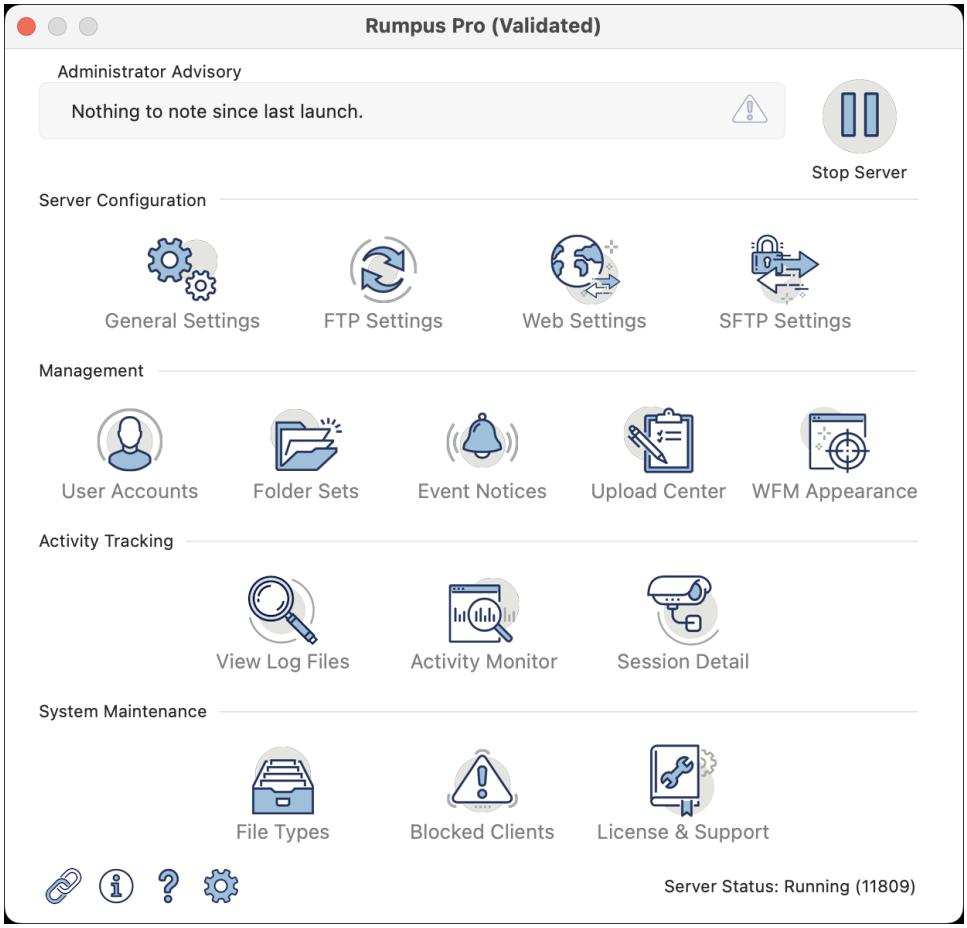
Rumpus 10: New Features

Contents

Modernized Administration Interface

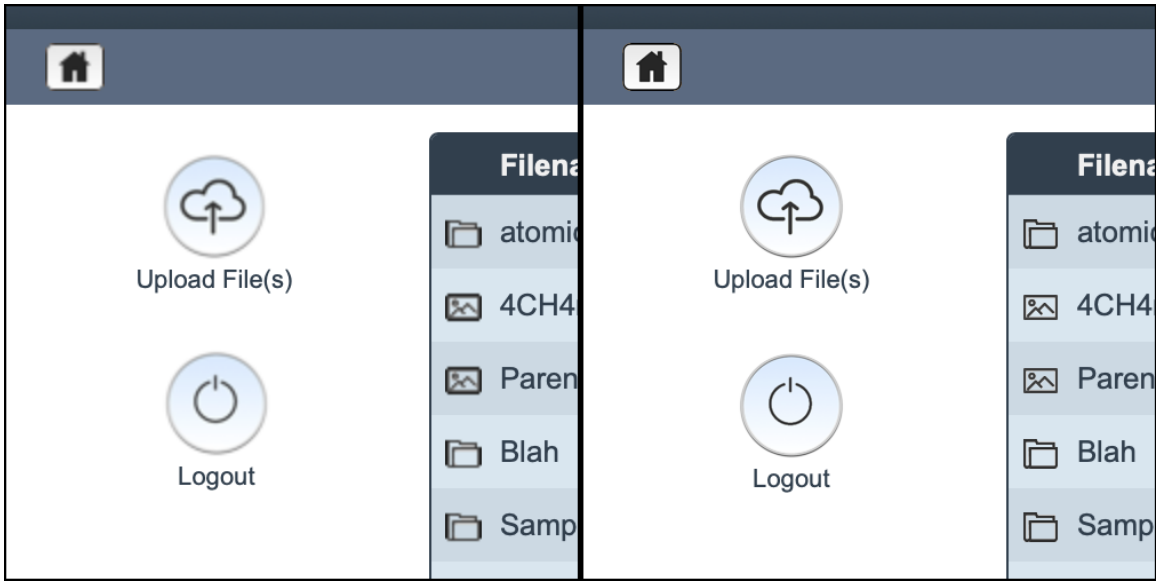
The Rumpus control application has been updated for easier navigation and fresh appearance.



Long time Rumpus administrators will find that the primary options are the same, for the most part, with some reorganization. In particular, SFTP settings have been moved to their own control window, and the Web server management has been split into 2 control windows. The "Web Settings" control window provides access to server-wide HTTP settings like authentication options, the Drop Box, and other core functions, while the "WFM Appearance" window provides controls for colors, fonts, layout options, logos, and so forth.

High Resolution Web Interface

The Rumpus Web File Manager is now offered with a high resolution appearance. The improved sharpness is most noticeable on mobile devices, but increasingly, modern desktop computers also have displays that dramatically improve the interface.



Standard Resolution Display **High Resolution Display**

High-resolution graphics require larger files and may slightly impact page loading times, but this difference is minor and in most cases is imperceptible. The only other drawback is that your logo file(s) and other supporting images may need to be updated for display at 2X resolution.

To enable the high-res display, simply check the "Use High Resolution Graphics" option on the "Display" tab of the WFM Appearance window.

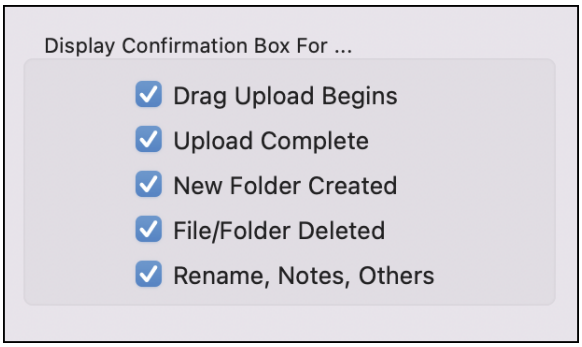
Important! Local Web browser caching may cause display issues when testing this feature and switching back and forth between the high-res and low-res interfaces. When loading the WFM interface in a test browser, be sure to use the browser's "Empty Cache" function to clear your browser cache after switching the resolution mode in Rumpus. In production use, the option will remain constant at either standard or high resolution graphics, so browser caches will work normally with a consistent appearance.

Workflow (Dialog Boxes)

The Rumpus Web interface is designed to be as clear to users as possible. For example, when a user drags a file from their desktop into the Rumpus directory display, an"Upload File" dialog box opens, showing the user the name of the file to be uploaded and allowing the user to confirm the transfer. When the transfer is complete, a message is shown to the user confirming that the file was successfully sent.

While these dialog messages make the process clear, they also require additional confirmation ("OK" clicks), slowing down user workflows. So on some servers, the administrator may prefer to skip some or all of these messages. In the case of a file upload, when a user drags a file from their desktop, you might prefer that the file transfer start immediately, without the need of confirmation, and when the transfer is done you might want the user returned immediately to the directory listing (with the newly uploaded file included in the listing, of course).

On the WFM Appearance window, Display tab, a number of options are available that allow the administrator to choose which dialog messages are displayed, and which can be skipped.



As with the resolution setting, color selections and other appearance options, be sure to clear your browser cache and perform frequent browser reloads when testing this option. Changing any of these options won't effect Web browsers that have already loaded the WFM display, so a reload/refresh is needed.

Actions Menu Appearance

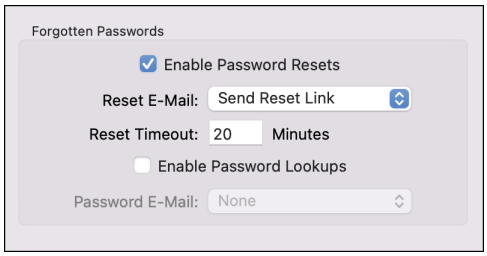
With the addition of high-resolution graphics, Rumpus also includes new options for the "General Actions" user functions. The General Actions are the buttons displayed in the Web File Manager that allow users to perform various tasks not related to a specific file.

The "General Actions" buttons are highlighted in the screen shot below.

The General Actions button appearance is configured on the WFM Appearance window "General Actions" tab. In Rumpus 10, new button styles are offered, and the buttons are available in a selection of colors to better integrate with the look of your Web File Manager service.

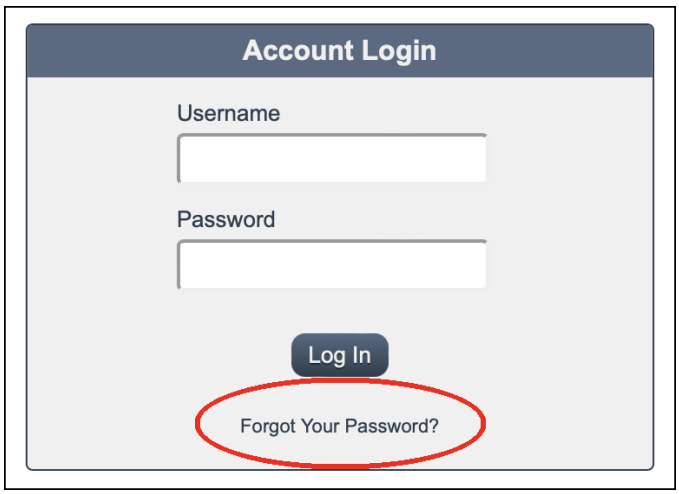
Password Resets

In past Rumpus releases, administrators could allow users to retrieve a forgotten password via e-mail. However, the preferred method of handing forgotten passwords is using an e-mailed reset URL, rather than simply reminding the user of their password. For Rumpus 10, password reset URLs can now be automatically generated and sent, improving password security. The new feature is managed on the Web Settings window, Authentication tab, using the Forgotten Passwords options.



To enable this feature, you'll first need to create an Event Notice that defines the reset e-mail to be sent. The Event Notice will be a standard e-mail notification, with a subject and message body customized as needed. Once you have created an Event Notice, open the the "Custom Message Body" sheet and from the "Event Type" menu choose "Password Reset". This will install a default message body that you can customize for your service.

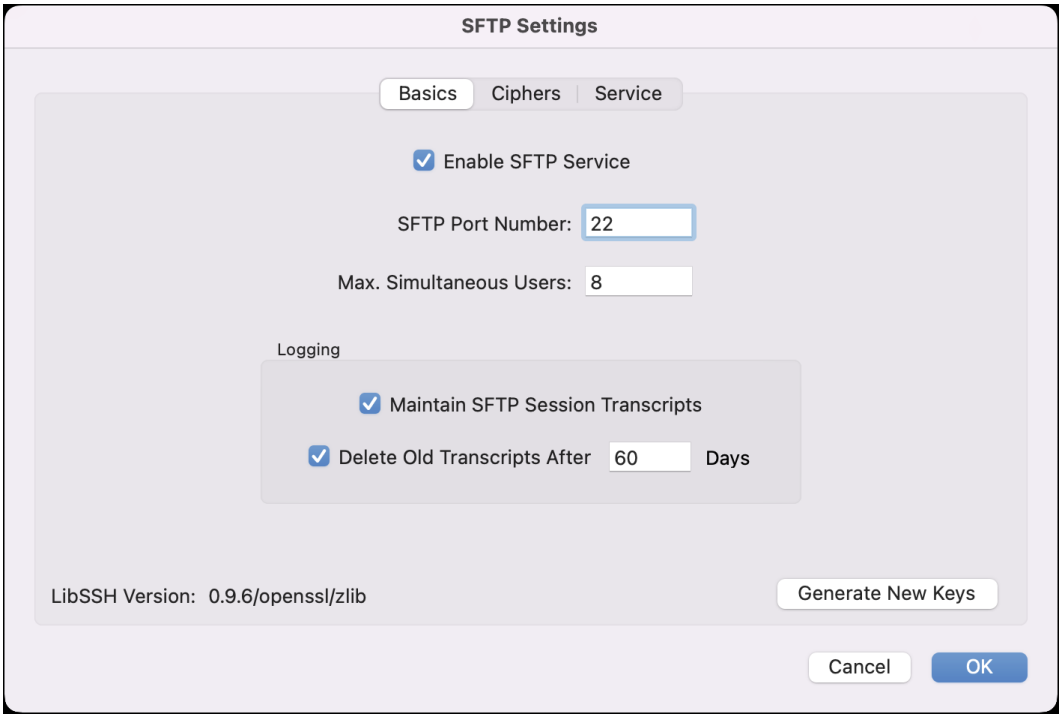
With the Event Notice created, turn on the "Enable Password Resets" option and select the notice to be used. The "Reset Timeout" specifies the amount of time allowed between a user requesting a password reset link and using it to complete the password change. The default of 20 minutes is usually sufficient.



Once enabled, a "Forgot Your Password" link will be included on the WFM service login page, which users can use to request the automated password reset link.

SFTP

The Rumpus SFTP service, once considered a feature of general FTP server management, has been elevated to a fully developed service that stands along with FTP, FTPS, HTTP, HTTPS and WebDAV. A new control window allows administrators to manage the service.



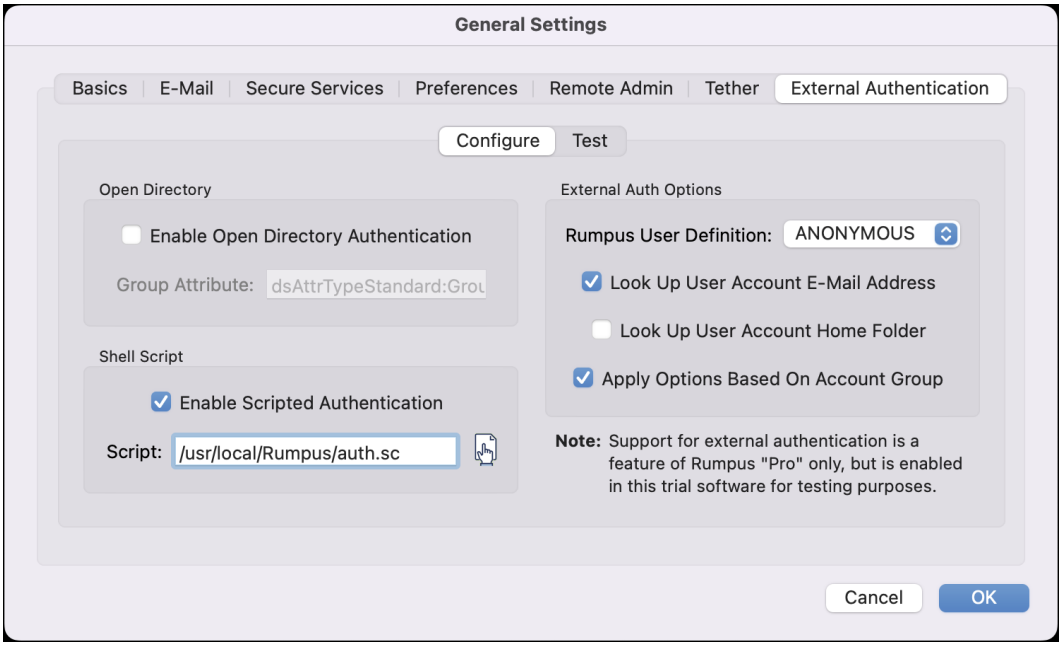
Most of the changes made in the SFTP service are in the server engine itself, improving both performance and stability. Security has also been improved, with administrators now able to select ciphers for either better cryptographic security or wider compatibility with older SFTP clients.

The most notable update, other than the improvements in the SFTP engine itself, is support for 2 factor authentication. Until Rumpus 10, 2 Factor Auth was possible only in the Web File Manager, and could not be deployed for the more fundamental file transfer protocols. On the SFTP Settings window, "Service" tab, administrators can now enable "Password Authentication" and "Public Key Authentication". Public keys can be applied on the User Accounts window so that connecting clients can be required to authenticate using a password, a stored key file, or both.

Scripted Authentication

In additional to maintaining user accounts within the Rumpus application, or via LDAP, Rumpus now offers a third option for user account management, authentication via shell script. Using scripted authentication, organizations can maintain user accounts in virtually any format, using a simple scripting system to confirm access to Rumpus services.

This feature, which is available in Rumpus Pro only, can be configured on the General Settings window, External Authentication tab, as shown.



When enabled, users who access the server via any supported protocol (HTTP, HTTPS, FTP, FTPS, SFTP or WebDAV) will be presented with the usual login prompt. The name and password supplied by the end user is then handed to a script created by the administrator, which can respond with acceptance or denial.

The shell script itself accepts the username and password as arguments 1 and 2, and responds with an XML-like "Allow" response of "true" or "false". Here is an example script that will allow access to the user account "SampleUser" when the password "ABC123" is applied.

```
#!/bin/bash
if [[ $1 == "SampleUser" && $2 == "ABC123" ]]; then
echo "<Allow>true</Allow>"
else
echo "<Allow>false</Allow>"
fi
```

For this example, assume the above script is saved in the file "/usr/local/Rumpus/auth.sc". As a test, the script could then be run from the command line like this:

```
/usr/local/Rumpus/auth.sc SampleUser BadPass
```

In this case, since the password (argument 2) is incorrect, the result would be:

```
<Allow>false</Allow>
```

Rerun the test with the correct password:

```
/usr/local/Rumpus/auth.sc SampleUser ABC123
```

and the result would be:

```
<Allow>true</Allow>
```

In production, when configured as the external auth script, the "true" result would indicate to Rumpus that the user should be granted access.

Successful authentication responses can optionally also include the user account home folder, e-mail address, and an applicable group, as in:

```
<Allow>true</Allow>
<HomeF>/Users/Shared/SampleUser/</HomeF>
<EMail>SampleUser@AcmeMail.com</EMail>
<Group>GuestAccess</Group>
```