What's New In Rumpus 8

Contents

Rumpus 8.2

Tether

Rumpus Tether is a brand new client application designed specifically for in-house users of your Rumpus file transfer server. It replaces the previous companion application Rumplet, as well as local uses for third party FTP/WebDAV client applications.

Using Tether, your local users (or remote users who also need dedicated server access) can view, upload, download, and manage files on the server, access files recently uploaded to their content area, and create and manage drop shipments. Tether's simple interface and Rumpus-optimized features are designed to improve workflow for your entire organization. While it is available as a separate download package, Rumpus 8.2 adds support for the Tether client application.

Two-Factor Authentication

For years, Rumpus has supported username/password authentication. Supplying a password is one way ("factor") that users can confirm their identity when logging into your server. For increased security, a second factor can now also be required.

When two-factor authentication is enabled, users must supply a PIN ("Personal Identification Number"), in addition to their password. The PIN is sent by Rumpus automatically via e-mail, thus confirming the user's identity by proving that they have access to their known e-mail account, as well as knowledge of their password.

Convenience and Security Updates

A variety of lesser changes and additions are included in Rumpus 8.2, including:

- Improved client tracking for servers behind reverse-proxies.
- Tracking of user mobile phone numbers (primarily in support of 2 factor authentication).
- The ability to require password protection for drop shipped files.
- Anti-robot support for Upload Center forms.
- "Administrator Advisories" to warn administrators of potential problems.
- Web file listing "key press auto-scroll".
- Security improvements, including "clickjacking" prevention.
- Updates to OpenSSL (1.0.2p) and LibSSH (0.7.7).
- The "CipherListCustom" conf directive allows administrators to specify the exact TLS cipher list.

Rumpus 8.1

Improved Server Security

Security has been a major focus for this release of Rumpus, and version 8.1 offers several significant feature updates to keep your server safe, including:

- OpenSSL has been upgraded. The update not only takes advantage of updates in the OpenSSL 1.0.X branch, but incorporates improved support for TLSv1.1 and TLSv1.2. Administrators can now optionally disable TLSv1.0, TLSv1.1 and SSL/TLS Compression. By default, Rumpus also supports an updated list of ciphers that maximizes compatibility with slightly-out-of-date clients while ensuring the highest practical level of encryption between client and server.
- Users can now be required to change their passwords periodically, and password strength requirements can be enforced by Rumpus. Also, users logging in for the first time can be required to set a new password.
- In the SFTP service, we've added the ability to use private/public key authentication, in addition to username/password authentication. It's a very handy feature for clients that need to regularly transfer files with maximum security. For details, see the article "SFTP" section of the Secure Transfers article in the download package.
- On servers that require all Web users to connect securely (via HTTPS), HTTP Strict Transport Security can now be enabled.

The Web File Manager "Basket"

The Rumpus "Basket" is a useful feature, especially for those who use the Drop Ship function extensively. In essence, the feature allows users create a collection of files and then process the collection in a single action. Users can move from folder to folder within their content area, adding files to the basket as they go. The basket can then be drop shipped in a single drop ship URL, moved to a set destination folder, etc. In the case of a drop shipment, when a basket of files is sent, the recipient accessing the drop ship URL sees each file sent and can view or download the files as needed.

Improved Media Display

Rumpus is increasingly used to display images, video and audio, so Rumpus 8.1 includes a more flexible mechanism for displaying media files in the WFM interface. The Web display of numerous content types have already been optimized, and the new display mechanism will allow Maxum to continually improve the display interface of individual content types in the future

Additional Helpful Administrative Updates

User accounts with passwords assigned can now also be assigned an SMTP password, allowing Rumpus to send mail natively as individual users. The SMTP port can now be explicitly assigned in Event Notices, making SMTP settings easier to configure. Rumplet can now send files to the Rumpus server via an available HTTP connection, allowing users not on the local network to effectively use the Rumplet application. WebDAV client compatibility has been improved. Files uploaded from mobile devices (in particular, Safari on iOS) can now be sequentially named so that multiple files can be uploaded from the device at once. An option to roll logs into a zip archive rather than simply copying files helps keep historical archives better organized and consume less disk space.

Rumpus 8.0

Rebuilt Web File Manager

The Rumpus Web File Manager (WFM) has been rebuilt from the ground up to be easier to use, more flexible, more efficient and include new features. Almost every element of the Web interface is now customizable right from within the Rumpus application, for example:

- File and folder menus are now completely customizable, and the same menus are displayed in both standard and thumbnail directory listing views.
- Setup wizards allow administrators to quickly define color pallets and basic options, and then individually fine tune the display of dozens of different elements.
- Action buttons can be displayed in different styles, with more fine tuning controls, and in different positions within the interface.
- Progress indicators have been simplified and improved, and can now be displayed for file downloads as well as uploads.
- The data required to deliver Web interface pages is up to 50% less than in past versions, while being presented in a more modern, cleaner style.
- For Drop Ship users, the new Web interface includes a drop ship history, allowing senders to view past shipments and easily copy/paste previous URLs for resending.
- Users can now move files between folders, without transferring them to and from the server.
- Video files can be displayed in a branded display interface which includes a "Download Now" option for permanent retrieval of the file.

SFTP Service

Rumpus now supports SFTP clients, in addition to HTTP, HTTPS, FTP, FTPS and WebDAV. User accounts and restrictions are applied just as they are in any other protocol. Just turn on SFTP service in Rumpus (a 10 second task) and your clients can use any standard SFTP client to transfer and manage files.

New Event Notices

New Event Notice types can save text or XML files when users upload files. Handy for use along with Upload Center forms, this makes it easy to prompt users for information about uploaded files and record meta-data about uploaded files.

Auto-Complete Form Fields

Administrators can now create lists, which can be used in form text fields as prompts for users during data entry. For example, you might create a list of all the e-mail addresses of people in your company, and assign it as an auto-complete list for an "e-mail" Upload Center field. Auto-complete lists can also be applied to File Request and Drop Ship mail fields, making it easier for local users to address messages sent by Rumpus.