

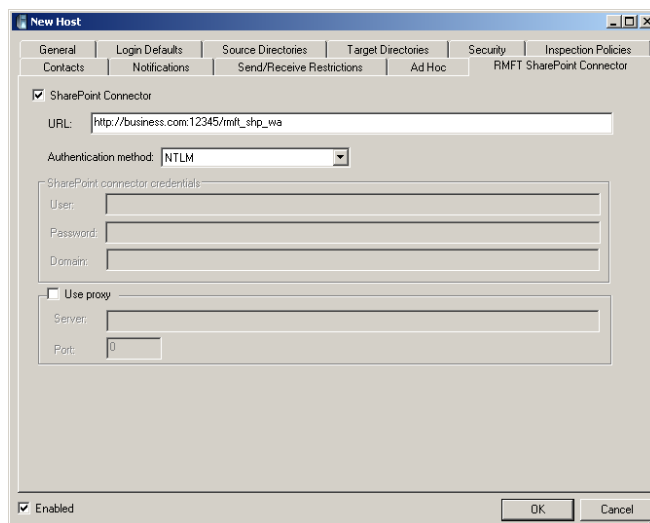
## RMFT 2.4 – Release Notes November 2008

RMFT allows organizations to architect efficient workflows and facilitates user-friendly file exchanges so IT resources can focus elsewhere. As a secure communications platform, RMFT offers key features such as authentication, file access authorization, encrypted transport, and comprehensive auditing over the file transfer process. As an automation solution, RMFT allows organizations to schedule and execute end-to-end transfer processes with guaranteed delivery using standard and/or proprietary protocols.

RMFT 2.4 introduces a host of new and improved features, among them, the ability to pull/push files from/to SharePoint sites (either automatically or user-initiated); RMFT Desktop Client, a fast and convenient method of sending files using the Windows Explorer right-click menu or drag-and-drop; white lists for ad hoc user creation and improved notification/audit information.

### New and Improved Management Capabilities

**SharePoint® Integration** – RMFT’s transfer automation capabilities have been extended to support pull and push of files from/to SharePoint Sites. SharePoint integration has also been added to RMFT Shared Folders, enabling RMFT Web Client users to transparently upload/download files to/from SharePoint sites, *without requiring SharePoint access rights*.



**Notification on Sender’s Behalf** – New package notifications and ad hoc user invitations/enrollment requests can now be sent on behalf of the package sender rather than from the system.

**White Lists for Ad Hoc User Creation** – The current functionality of restricting ad hoc user creation by blocking certain email addresses/domains has been extended

to incorporate white lists. Administrators can now restrict the creation of Ad Hoc user accounts by only allowing certain email addresses/domains. This is useful for organizations who only want to allow ad hoc user creation for a limited number of domains or for administrators who want to block domain-specific users while allowing the creation of other ad hoc users belonging to the same domain.

**Reflecting Notifications Failures in Final Package Status** – Administrators can now determine whether the final package status will reflect package notification failures (for packages which were transferred successfully). If this option is enabled, packages with notification failures will be displayed in the Package Monitor with a “warning” icon.

**Extending Expiration of Pulled Packages in the Event of Failure** – When this option is enabled, the expiration period of a pulled package that cannot be delivered to its recipients, will be automatically extended by the specified number of days. This will allow RMFT administrators to resolve the delivery problem before the package expires.

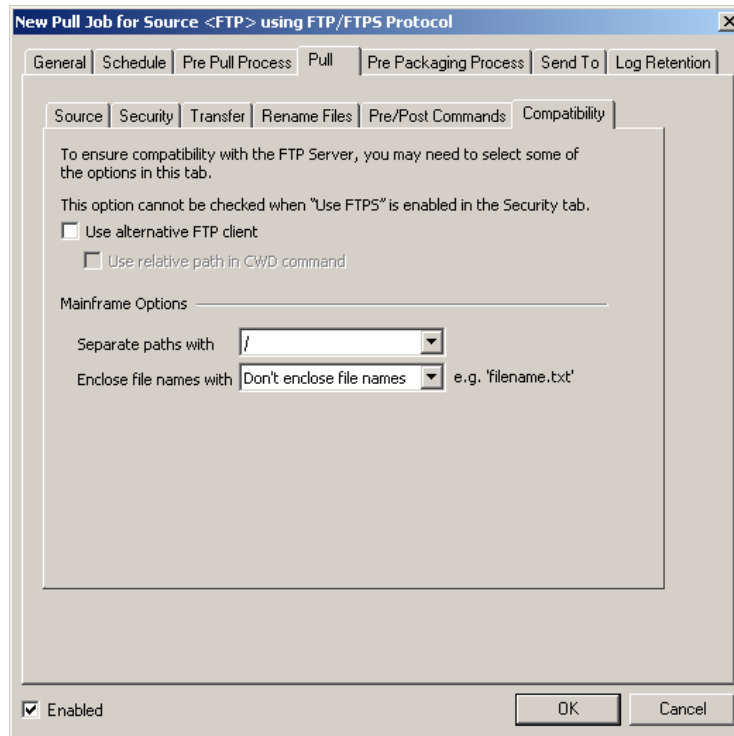
**New Warnings and Alerts** – Extended monitoring capabilities enable RMFT Administrators to be notified when any of the following situations occurs:

- **Insufficient disk space** - A warning will be shown in the System Health Monitor if disk space falls below the specified minimum.
- **Expiration/Notification process stops** - A warning will be shown in the System Health Monitor if the Expiration/Notification process stops.
- **Files remaining in Hot Directories** - When using SMB – Hot Directory protocol, a warning will be reported to Event Viewer if files remain in Hot Directories for longer than the specified time period.
- **Critical system problems** - You can request to be notified if a critical system problem occurs. The e-mail message will describe the nature of the problem.

**Outbox Purging** – To preserve disk space, incomplete packages (caused by interrupted transfers) are now automatically purged from outboxes according to the specified frequency.

### FTP/FTPS Improvements –

- A new **Compatibility** tab has been added to FTPS/FTPS protocol, enabling transfers to and from MVS mainframes as well as other types of FTP Server.



- A **Continue even if files are missing** option has been added to the FT/FTPS **Source** tab. When this option is selected, the transfer will occur even if not all the files listed in the List File are present in the source directory (and the job will end with success).

**Database Credentials Utility** – The Database Credentials Utility enables RMFT administrators to change the credentials that RMFT Server uses to connect to the RMFT database. This may be necessary if corporate security policies require the database password to be changed periodically.

**Automatic Load Control** – Automatic Load Control ensures that RMFT Server remains responsive even when large numbers of jobs are being processed. Load Control is activated when the system load reaches a user-definable number of jobs. There are three levels of load control: light (activated when 75 jobs are being processed), heavy (activated when 100 jobs are being processed), and maximum (activated when 125 jobs are being processed). RMFT Server responds to load control by holding some jobs while allowing others to complete (heavy load control) or by preventing the creation of new jobs (maximum load control).

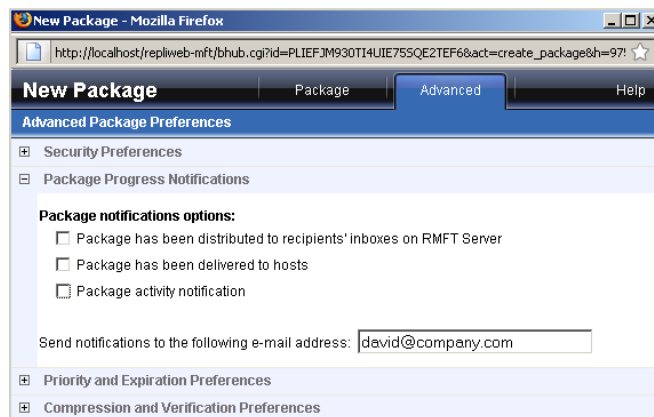
**Database Credentials Utility** – The Database Credentials Utility enables RMFT administrators to change the credentials that RMFT Server uses to connect to the RMFT database. This may be necessary if corporate security policies require the database password to be changed periodically.

**Run Instance Now (Previously “Submit Now”) Improvements** – The **Run instance now** option (previously available only for Scheduled jobs) now lets you run an immediate instance of Holding and Outside Timeframe jobs. In addition, running an immediate instance of a job will not affect the original scheduling parameters.

## New and Improved End-User Capabilities

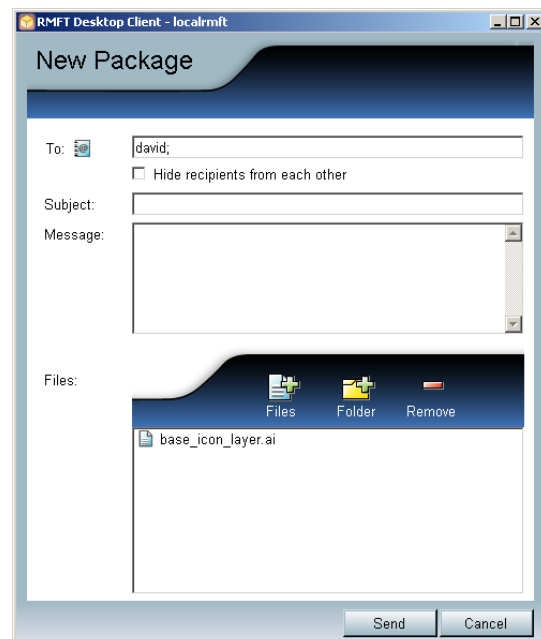
### New Package Notifications

– Senders can now request to be notified whenever a recipient opens the package or downloads any of the files. A final notification will be sent before the package expires summarizing the recipient activity. The new notification events are also reflected in the package audit trail display, which has been enhanced to show which of the recipients opened the package, which recipients downloaded files, and which files each recipient downloaded. The date and time of each event is also shown.



**Private Package** – Senders can now hide package recipients from each other. This is useful if the sender does not want each recipient to know that the package was also sent to other recipients.

**RMFT Desktop Client** – An integral part of the RMFT product suite, RMFT Desktop Client enables RMFT users to send any number of files to each other or to Ad Hoc users (if allowed) by simply right-clicking the selected files in Windows Explorer and selecting **Send to Recipients**. Support for server-side profile configuration enables administrators to provide RMFT Desktop Client users with the ability to start sending files “out-of-the-box”.



Other features include:

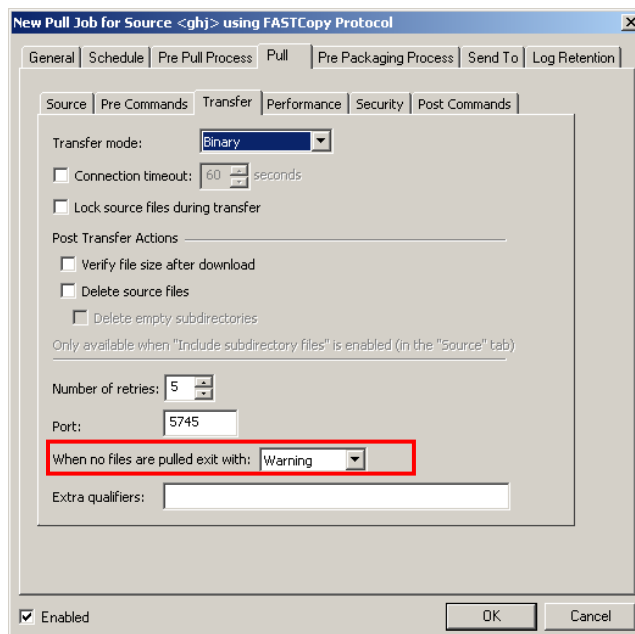
- Multiple provisioning options (for making RMFT Desktop Client available to Users)
- Multiple connection options (secure and non-secure)
- Integration with MS Outlook 2007 address book
- Unlimited file size and amount
- Drag and drop files and folders from Windows Explorer to RMFT Desktop Client
- Powerful virtual Explorer layout lets users drag and drop files and folders within the RMFT Desktop Client interface, enabling them to manipulate the package structure as required
- Simple to set up "Profiles" enable users with multiple RMFT accounts to switch between accounts as required

**RMFT Web Client Language Support** - RMFT Web Client now comes with four built-in languages: English, French, Spanish and German. RMFT administrators can change the order in which the languages appear in the Login Page as well as the number of languages, as required.

## Known Issues

- The total size of files that can be transferred using SCP protocol cannot exceed 1.2 GB.
- Download from SharePoint sites using RMFT Web Client in Java mode is currently not supported.
- In RMFT 2.4, additional proxy options (such as authentication) have been added to HTTP/S host protocol (source and target). A check box has also been added to enable or disable the use of a proxy server. When upgrading to RMFT 2.4, the **Use proxy server** check box (in the **Transfer** tab) is added *unselected*. If you used a proxy server in the previous version and you want to continue using a proxy server, you will need to select the check box.
- When pulling files from a host running an incompatible FASTCopy Receiving Agent, the job may end with a parsing error if the **Success** or **Error** options are selected and no files are pulled. If the default **Warning** option is selected, the job will complete with a warning if no files are copied. If you want the job to end with **Success** or **Error** when no files are pulled, you will need to upgrade the FASTCopy Receiving Agent on the source host to a compatible version (RMFT 2.3.307 and above).

On UNIX platforms FASTCopy version 2.6.3.5 or higher is supported. To find out which FASTCopy version is installed, open a UNIX shell and run the command `fcopy -info` or `fcopyd -info` (`fcopyd -info` will not work if an `fcopyshr` patch was applied to the version).



## Bug Fixes

The following is a list of issues that have been resolved in RMFT 2.4:

- When an internal exposed user invited an external Ad-Hoc user, the status of the user on the DMZ RMFT Server would remain "Pending", even after the user accepted the invitation.
- On Windows 2003, Logging in to the Web Package Monitor with IE 6.0 and pressing the "Filter Settings" button would generate the following Java script error: "connection\_id is undefined."
- After reinstalling the external RMFT Server, when viewing package information on the internal server, the audit trail would not show external packages (only internal).
- When an external user would send a package to an external host and request to be notified on delivery to host, a redundant notification would be sent confirming delivery to the system host.
- Package distribution to distribution lists containing hosts with no default targets would finish without an error, despite the system's inability to deliver the package to these hosts.
- The SuperFAST Scenario log did not specify the cause of the error when a transfer error occurred due to insufficient hard drive space.
- When trying to view a package's delivery details, a logon error message would appear if the **Save Password** check box was not selected in the connection manager.
- In the case of a FASTCopy authentication failure, the error was not specific enough.
- RMFT and R-1 Coexistence - Updating RMFT's FASTCopy license would not update the RMFT FASTCopy license inside the RDS folder.
- The number of retries for the FASTCopy DMZ pull job was set to 100. If the pull job failed and the failure was *not* due to a connection error, the failure would only be made apparent after the retries completed.
- File sizes over 2GB were not displayed correctly in the delivery audit trail.
- If the RMFT system credentials were changed, newly issued child job instances would attempt to run under the old credentials and fail as a result.
- Backslashes could not be used in the FASTCopy password.
- After a FASTCopy pull job ended, the parent job's scenario.log would sometimes be locked. When this happened, the job would end successfully, but the created package would not contain the pulled files.
- In RMFT Manager, the **Next Scheduled** column was sorted as string.

- When using the Web Client in Lite mode, there was no option to upload files from an UNC path.
- RMFT Web Client (ActiveX) would encounter a problem when sending a package with 1000 files using an untrusted certificate.
- Web package monitor would produce a JavaScript error when opening the filter settings.
- When choosing the **Disable accounts if not active for...** option, the notification/expiration job would fail.
- FASTCopy Pull/Push would fail when using the host Login Defaults and the credentials contained special characters (e.g. a comma).
- The internal sorting of a package pulled from the outside and the rest of the delivery family that it created would ignore the pull definition for log retention and use system default instead.
- Inbox processing would retry in an infinite loop if the number of retries was set to zero.
- Installation of RMFT Desktop Client on Vista64 would fail.
- Log retention would erase the wrong jobs when the maximum number of instances was reached.
- Inspection policy settings were not propagated to exposed users/hosts on the external server.
- Even though RMFT Web Client is configured to use HTTPS only, the link to the Recipient Activity Report would use HTTP.
- Web customization did not support hiding the "More" button in the **Package Details** screen.
- The ~RepliWeb\RMFT\web\b-hub\customizer\default.xml file would be replaced during upgrade.
- Users would be created with Password Expiration = "Never" instead of "Use Defaults".