RMFT
Managed File Transfer

RepliWeb

RMFT 2.4.3 Release Notes
October 2010

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 2.4.3 introduces several new features as well as improvements to existing features. Console administration improvements enable administrators to quickly locate relevant packages and review package audit events. A new Java SDK facilitates seamless integration of RMFT's client and auditing capabilities with other applications. Enhanced support for corporate installation procedures enables smooth and rapid deployment of RMFT components within the organization. The end-user experience is now even more versatile with the addition of new login options. Additionally, RMFT 2.4.3 has been reviewed and accredited by a leading information security firm.

Key features include:

- A redesigned Package Audit interface, enabling RMFT administrators to easily review package events and troubleshoot any problems.
- New "Operator" role enabling authorized Windows users to monitor RMFT jobs and package transfers.
- Shared RMFT Desktop Client profiles for easy distribution within the organization.
- Silent installation of RMFT Desktop Client and other RMFT components.
- Java SDK for integrating RMFT's package sending and auditing capabilities into third-party applications.
- Package auditing capabilities has been added to the RMFT .Net SDK.
- Public links, private links and recall functionality has been added to the RMFT .Net SDK and the RMFT Web Services.

Significant improvements have also been made to stability and performance.

For more information about a particular feature, please refer to the *RMFT Administrator's Guide*.

Monitoring and Auditing

RMFT Manager - The new Package Audit interface (shown below) provides RMFT administrators with a detailed report of the events that occurred both during (server events) and after (recipient actions) package processing.

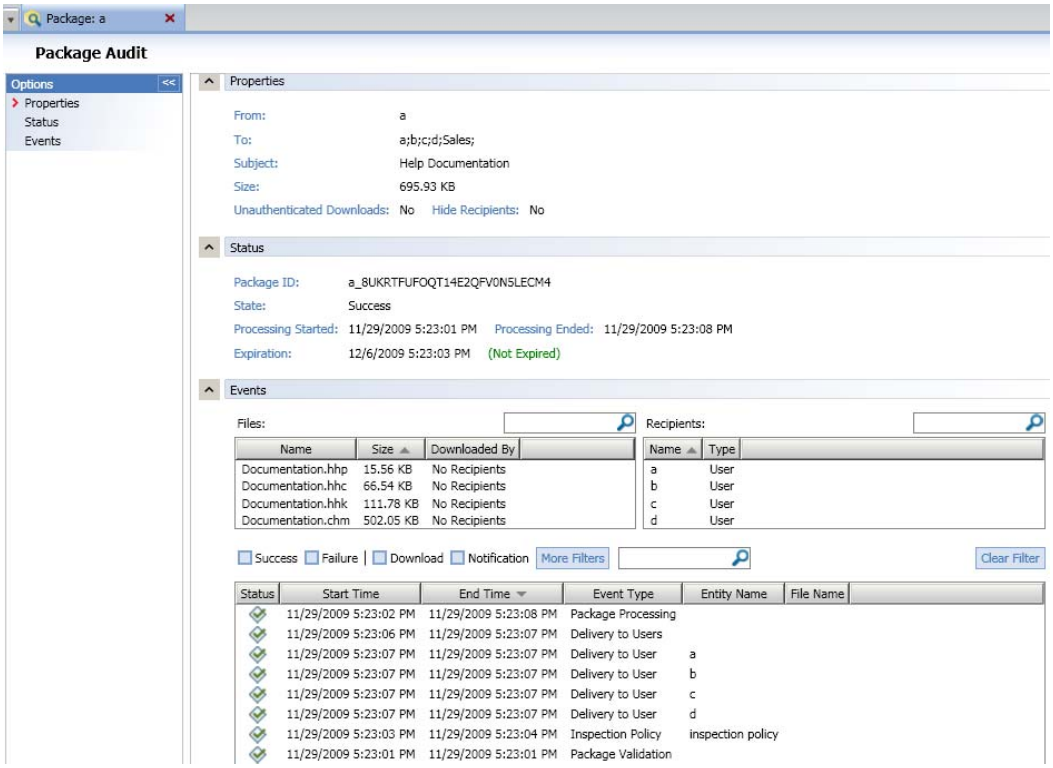
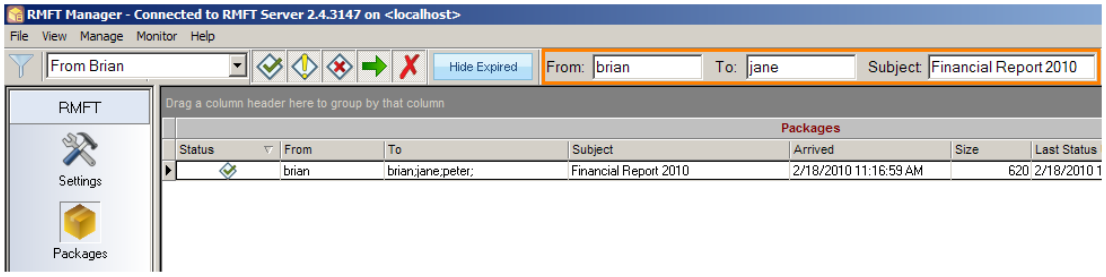


Figure 1: New Package Audit Window

Quick Filter Toolbar – Package filtering has been enhanced through the addition of a Quick Filter Toolbar to the **Packages** pane. Using the Quick Filter Toolbar, administrators can quickly find relevant packages by overriding the **From**, **To** and **Subject** settings of the currently selected filter.



POP3/IMAP - An option to include a message's .eml file and its attachments in the package has been added to the **Include** tab of POP3/IMAP protocol. The .eml file contains all of the message properties such as who sent the mail, the CC recipients and more.

Heavy Load Reporting - RMFT Server maintains responsiveness by automatically activating load control when the number of active Jobs reaches a predefined threshold. RMFT will report to Windows Event Viewer if Heavy Load control is active for longer than a predefined time period. After the initial report, it will continue reporting at regular predefined intervals until Heavy Load control is deactivated (which will also be reported). The default reporting intervals can be changed by editing the `[Load Control]` section in ~\RepliWeb\RMFT\scheduler\config**server.conf**

RMFT Client SDK and Web Services

This version includes a Java SDK for integrating RMFT's package sending and auditing capabilities into third-party applications. The Java SDK complements the .NET SDK whose existing functionality has been extended to support package auditing.

Additionally, the RMFT Web Services and .NET SDK has been expanded to include the following capabilities.

- **Private Links:** Allows the creation of separate (i.e. unique) download links for each of the package files according to the number of recipients enabling senders to know which recipients downloaded the files.
- **Public Links:** Enables the creation of a download link for each of the package files but, unlike private links, public links are not recipient-specific. When files are downloaded by clicking on public links the downloader's identity remains anonymous.
- **Recall:** Enables sent packages to be marked for immediate expiration.

Installation and Upgrade

Silent Installation - Silent installation of RMFT components has been expanded to support RMFT Receiving Agents, RMFT Desktop Client and the RMFT Administration Console.

Upgrade to 2.4.3 - In RMFT 2.4.3, the package auditing information has been extended to include additional package events. These changes affect both the backup procedure and the related upgrade procedure.

- **Backup** - Before beginning the upgrade, use the modified backup utility provided with the RMFT 2.4.3 installation kit to back up your existing packages and settings. For information on replacing the backup utility, please refer to the readme file. Note that if you back up your packages and settings using the existing backup utility, the additional auditing information introduced in RMFT 2.4.3 will not be available for restored packages.
- **Database Upgrade** – During upgrade, the existing RMFT database tables will be modified to support the new auditing information. Setup will calculate the estimated duration of the database modification process. If it is estimated to take more than 10 minutes, you will be asked whether

you want to continue the upgrade or perform the upgrade later (when there is less system activity).

FTPS Security and Transfer

Security – The addition of several new security protocols (SSLv2, SSLv3, SSLv23, TLSv1), ensures compatibility when transferring files to/from FTP servers

Transfer – The **Transfer** tab now includes a **Send "Keep Alive" command every [ ] seconds** option, enabling uninterrupted transfers of large files.

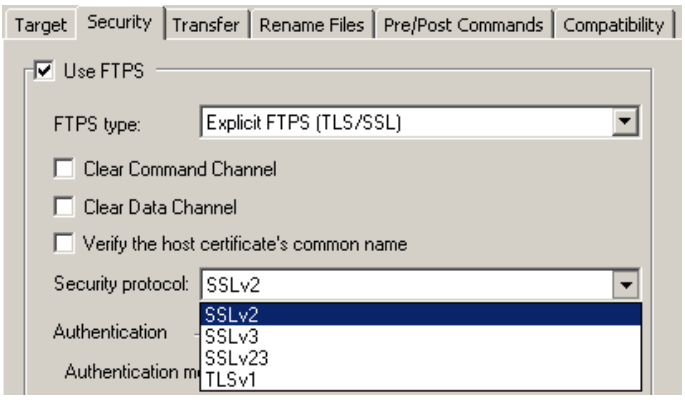
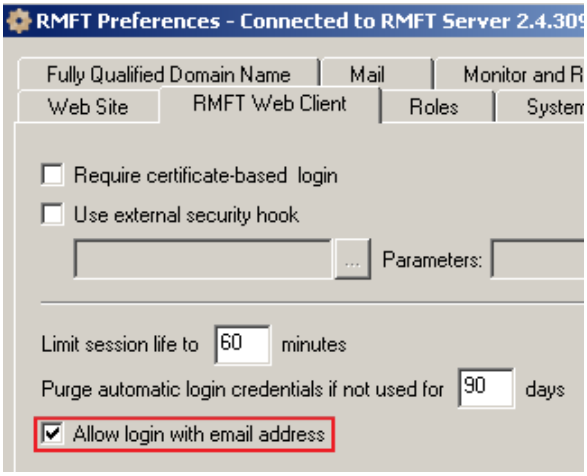


Figure 2: New FTPS Security Protocols

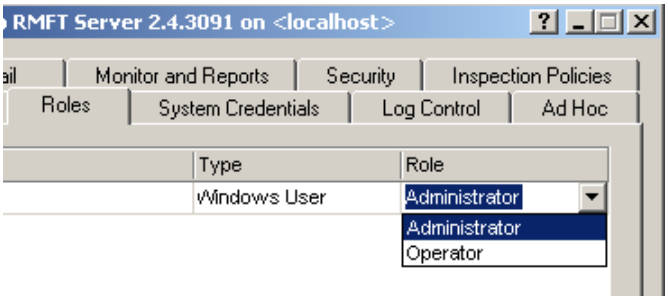
Email Login

To further enhance the user experience, users whose account settings include an email address can now log in with their email address as well as their user name. This requires the **Allow login with email address** feature to be enabled in the RMFT Web Client tab.



Operator Role

A new "Operator" role has been added to complement the Administrator and Group Administrator roles. RMFT Operators are able to perform monitoring-related tasks such as viewing, holding and aborting jobs and transfers.



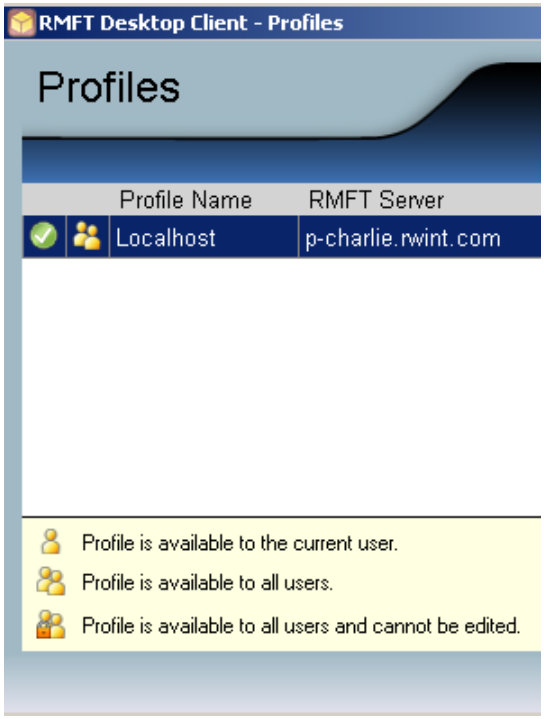
To reflect this change, the **Administrators** tab has been redesigned and renamed **Roles**.

Shared RMFT Desktop Client Profiles

RMFT administrators can now create RMFT Desktop Client profiles offline and then distribute them to computers within their organization using a suitable application (e.g. Active Directory). This is especially useful when performing a silent installation of RMFT Desktop Client (since the silent installation does not install any profiles). RMFT administrators can also prevent users from editing the shared profile by giving the profile file read-only permissions.

RMFT users can also create profiles and make them available to other users on the same computer by selecting the new **Shared profile** option in the **Edit/New Profile** dialog box.

The profile permissions are indicated by an icon (as shown in the image on the right).



Comprehensive Security Assessment

During the development of RMFT 2.4.3, RepliWeb enlisted the services of a leading security information company to perform a comprehensive security assessment of the application. The assessment was based on widely recognized standards, including those published by OWASP and NIST. The security assessment report concluded that RMFT 2.4.3 does not contain any vulnerabilities that could be exploited by an attacker to impact the integrity or confidentiality of the applications, application data, or client systems. A certification letter can be obtained by contacting support@repliweb.com.

Additional Features and Improvements

- Support for Windows Server 2008 R2 Cluster.
- Support for SQL Server 2008.
- Support for AES 256-bit encryption.
- Faster download speed in RMFT Web Client Lite mode.

Known Issues

The following is a list of known issues with RMFT 2.4.3. Where applicable, a workaround is provided to resolve the issue.

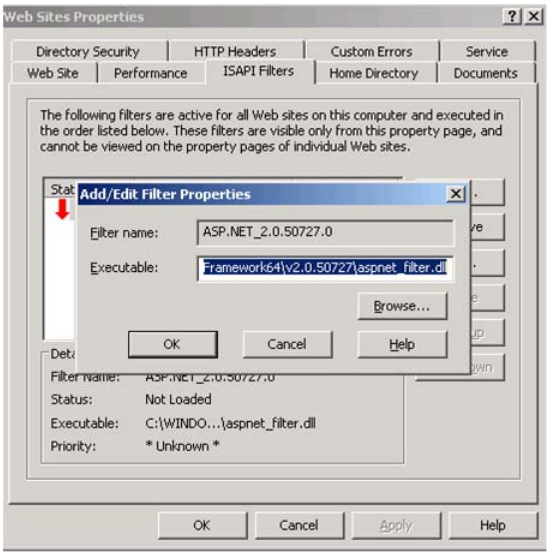
- **Google Chrome** - The RMFT Java Applet may fail to load when RMFT Web Client is run on Google Chrome for the first time. Pressing F5 will resolve the problem. (Although you usually only need to press F5 once, you may need to keep pressing F5 until the RMFT Java Applet is successfully loaded).
- **Oracle 11g Compatibility** – RMFT is compatible with the patched version of Oracle 11g. For information on which patch you need for your specific platform, you need to open a service request with Oracle Support for "patch 9064352 for <*platform*>" where <*platform*> is your OS and exact Oracle version (e.g. Oracle 11.1.0.7). You also need to attach the current list of one-off patches to the service request (obtained by running the `opatch lsinventory` command).
- **RMFT Web Site Support on 64-Bit Machines** – By default, the **RMFT Website** ISAPI filter on 64-bit machines is a 64-bit DLL. In order for the RMFT Website to work on 64-bit machines, the ISAPI filter path needs to be changed so that it points to the 32-bit DLL.

  Note: IIS cannot operate in 32-bit and 64-bit modes simultaneously. In other words, applications that require 64-bit functionality should not be run on the same IIS as the RMFT Web site.

To change the ISAPI filter path:

1. Open IIS.
2. In the left pane, right-click the **Web Sites** and select **Properties**.

   The **Web Site Properties** dialog box opens.
3. In the **ISAPI Filters** tab, click **Edit**.



4. In the **Executable** field, change the ISAPI filter path from:

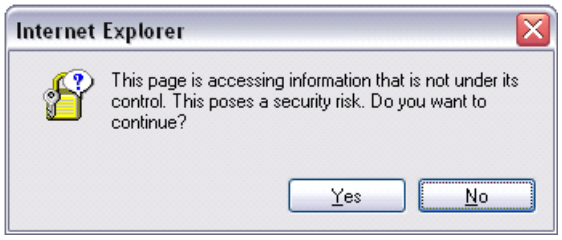
   ~\Framework64\v<*version*>\aspnet_filter.dll

   to:

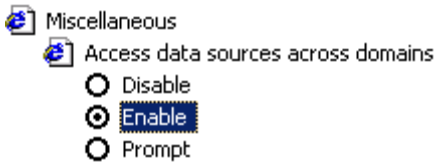
   ~\Framework\v<*version*>\aspnet_filter.dll

5. In the left pane, right-click **DefaultAppPool** and select **Recycle**.
6. Right-click **DefaultAppPool** and select **Stop**, then, right-click **DefaultAppPool** again and select **Start**.

- **IE6 on Windows Server 2003** – IE6 users may encounter the following error when attempting to log in to RMFT Web Client on Windows Server 2003:



To resolve this issue, users need to change the **Access data sources across domains** security setting to **Enable** (**Tools > Internet Options** > **Security** > **Select a Zone** > **Custom Level**).



- **"HTTP 413 Request Entity too Large" error** – Occurs when RMFT Desktop Client users try to send a package using "IIS Secure" mode or when RMFT Web Client users try to send a package using Java secure mode. This issue can be resolved by increasing the default IIS request size. For full instructions, please refer to:

  http://www.repliweb.com/resources/faq/managed_file_transfer/faq_531.php

- **Non-English Characters are Displayed Incorrectly** – RMFT Desktop Client and RMFT Web Client in Lite Mode both allow the sending of files whose names contain non-English characters. However, such files will not be displayed correctly in RMFT Manager (Package Audit) or RMFT Web Client (non-English characters will be replaced with random characters). This is also the case regarding non-English characters in the package subject and message.

  RMFT Web Client in Enhanced Mode does not allow the transfer of files with non-English characters in their names.

- **Reinstalling the DMZ RMFT Server to a Different Path** - In a setup involving an internal RMFT Server and a DMZ RMFT Server, the DMZ RMFT Server's installation path is stored in a configuration file on the internal RMFT Server machine. If, for whatever reason (e.g. hardware failure), the DMZ RMFT Server needs to be reinstalled, installing it to a different path requires you to also perform a special procedure. For detailed instructions, please refer to the *RMFT Product Suite Installation Guide*.
- **RMFT Desktop Client Installation Privileges** – RMFT Desktop Client installation privileges are environment-specific. For full details, please refer to the *RMFT Desktop Client Installation Guide*.
- **Incorrect "Delivery to Hosts" Status for Restored Packages** – The "Delivery to Hosts" event for packages restored from earlier RMFT versions may be shown as "Running" on the DMZ RMFT Server even though its actual status is "Success".
- **Usernames Containing Single Quotes** – Packages sent by users whose username contains single quotes (e.g. **mike'b** or **jane'''a**) cannot be downloaded using RMFT Web Client.

Bug Fixes

The following issues have been resolved in this version of RMFT 2.4.3:

- Upgrade to 2.4.3162 on Windows 2008 would fail during the database upgrade stage.
- The "'Recipient Activity Report' notification contained an invalid URL.
- RMFT scheduled jobs were not sensitive to time zone/daylight saving time changes.
- When accessing the RMFT web site for the first time, the following error would sometimes be displayed: "The server-side file Default.xml which is required to view RMFT Web Client pages is currently unavailable".
- Automatic Login would not work when clicking the Package Audit Link in the Recipient Activity notification.
- A checksum error would sometimes occur when downloading a file from RMFT Web Site using ActiveX.
- One of the Web Client errors contained the user's password.
- RMFT Web Client sometimes caused the IIS process to consume a lot of resources.
- When opening the RMFT Web Site from a link in another web page, the RMFT login page would sometimes try to close the browser.
- Packages encrypted with the RMFT certificate failed during processing on RMFT Server (ActiveX).
- FTP/S jobs using certificate authentication would fail sometimes.
- The Terms of Use notice was not displayed properly in the RMFT Web Client login page.
- Packages would sometimes stay in the running stage.
- Non-English file names were not displayed correctly in the package monitor.
- The Scheduler component would sometimes spawn many jobs and slow down the server.
- Obsolete records were not removed from the database.
- A checksum error would sometimes occur when downloading a file from RMFT Web Site using ActiveX.
- Sending a package to a large number of recipients using RMFT Web Client would sometimes not work.
- The CLI qualifiers `-before` and `-after` did not work.
- FASTCopy transfer in ASCII mode sometimes generated a corrupted file on the target.
- Lite users could not send packages to Distribution Lists with spaces in their name.
- File spec wildcards would not work when sending a package with the RMFT Java CLI.

- The fcopyd.exe process would sometimes stay alive and lock files, even when the session was disconnected.
- Safari would stop responding when clicking 'Done' or 'Cancel' in the Create Package window
- Users of the "Domain Users" group were sometimes not synchronized during the AD Sync process.
- Processing packages with a large message would sometimes crash the Oracle ODBC driver and the RMFT Monitor service.
- Lite users could not access the web site for the first time when clicking a link received in email notification.
- The number of internal retries for jobs was reduced from 100 to 10. This does not affect the number of retries set in the Manager GUI which relates to ….
- The maximum number of retries for FASTCopy/SMB/HTTP jobs was increased from 50 to 999.
- Support for wildcards was added when downloading packages using the CLI.