Release Notes

Product: RiskMan

Version: 2503

Overview: This document describes all enhancements and fixes made to RiskMan version 2503 (20 March 2025)

Last Updated: 20 March 2025

Table of Contents

Introduction

This document supplies an overview of new features, and enhancements to existing features, included in RiskMan version **2503**. The earlier released version of RiskMan was 2501.

All new features introduced in a new version of RiskMan are turned OFF by default, unless stated otherwise. This allows for decision to adopt new features, decide who will use the new features and complete change management tasks.

Should you have further questions about the content of this document, please contact RiskMan Support on **1800 018 984 (Outside Australia: +61 (0) 391 257 670)**, or via Customer Portal

If you would like to enquire about formal training for any of the features listed in this document, please contact the training team on **+61 3 9686 0009**, or via email: training@rldatix.com.

Application Management

Security Testing

Each release is subjected to automated testing against the 10 known Open Web Application Security Project (OWASP) security vulnerabilities. The top 10 known OWASP security vulnerabilities can be viewed here https://owasp.org/www-project-top-ten/

In the event of a High rated outcome, RLDatix undertakes a risk assessment to ensure any resolution implemented will not result in a negative impact on the application. The vulnerability will either be resolved prior to release, or if unable to be resolved, the vulnerability will be internally managed on the RLDatix APAC Risk Register.

If the event of a medium outcome, then RLDatix will work to resolve the vulnerability, where possible prior to release or if unable, then the vulnerability will be placed on the development pathway.

If the event of a Low or Information Only outcome, RLDatix consider the applicability and if to be resolved included on the product roadmap for future development.

Regression Testing

Regression testing occurs prior to every release and focuses on the likelihood that Bugs may have been reintroduced into the latest version.

Any reintroduced Bugs are resolved, or the feature disabled to enable release, and the Bug managed as part of the development pathway.

Functionality Testing

Functionality testing is completed by RLDatix employees to ensure that all features are working as expected. The results are reviewed, and any issues are resolved prior to release.

Enhancements and Changes

Enhancements and changes are rated on a scale of 1 to 3 by their significance and need for training. Some enhancements and modifications made to existing system features might be invisible

Significance Scale Explanation

▪ ▪ ▪	A small change that would scarcely be noticed, or something has been made much easier than before
▪ ▪ ▪	A significant change: expansion of existing functionality that may change the way you use the system
▪ ▪ ▪	A major enhancement or modification that would require proper planning to be rolled out

Need for Training Scale Explanation

▪ ▪ ▪	Users may only need to be told about the change; intuitive and simple, so usually no training required
▪ ▪ ▪	A change that will likely require internal training to ensure proper use; you may pick it up yourself
▪ ▪ ▪	A change which is highly involved and is likely to require RiskMan training in its proper use

RiskMan

New Features and Changes

Enhanced the email sending functionality to introduce an additional email sending option for "Microsoft Graph (Azure)" for use with OAuth permissions/security (where possible, it is recommended to use this option) and enable "MailKit" to work with OAuth permissions/security on the mail server.

The ability to configure OAuth within the global settings has been introduced as Microsoft have announced they will be permanently removing support for Basic Authentication for SMTP from September 2025 (ie the use of just a username and password to be able to send emails as is currently set up in RiskMan), which will impact those clients who currently use a Microsoft server for emails (this includes Office365). **Click here** for further details

Additional Global Settings to cater for OAuth:

- Mail | 10) Email Sending Method - additional item for Microsoft Graph (Azure)
- Mail | Mail Configuration | Mail Server Client ID for OAuth

This setting is the Client ID from the Mail server when using the OAuth authentication method. This is a requirement for using Azure mail servers without using BASIC authentication. Basic authentication is due to be deprecated on Azure mail servers so this will be a mandatory. To work, all 3 OAuth values need to be supplied, ClientID, TenantID and ClientSecret, and SSL/TLS must be enabled.

- Mail | Mail Configuration | Mail Server Authentication Authority for OAuth - This setting the authority provider details when retreiving a token for the OAuth authentication method when using Mailkit. When left blank, a value suitable for Office365 will be generated. This will be "https://login.microsoftonline.com/{TenantID}" where the TenantID is inserted. For servers other than Microsoft, the entire authority value must be provided. For GMail servers, for example, the value would be expected to be "https://accounts.google.com/o/oauth2/auth"

- Mail | Mail configuration | Mail Server Tenant ID for OAuth - This setting is the Client ID from the Mail server when using the OAuth authentication method. This is a requirement for using Azure mail servers without using BASIC authentication. Basic authentication is due to be deprecated on Azure mail servers so this will be mandatory. To work, all 3 OAuth values need to be supplied, ClientID, TenantID and ClientSecret, and SSL/TLS must be enabled

- Mail | Mail Configuration | Mail Server Secret for OAuth - This setting is the Secret from the Mail server when using the OAuth authentication method. This is a requirement for using Azure mail servers without using BASIC authentication. Basic authentication is due to be deprecated on Azure mail servers so this will be mandatory. To work, all 3 OAuth values need to be supplied, ClientID, TenantID and ClientSecret, and SSL/TLS must be enabled

- Mail | Mail Configuration | Mail Server Scope for OAuth - This setting is the Scope from the Mail server when using the OAuth authentication method. The scope describes the type of access token being requested. Please do not alter this without consultation. This is a requirement for using Azure mail servers without using BASIC authentication. Basic authentication is due to be deprecated on Azure mail servers so this will be mandatory. To work, all 3 OAuth values need to be supplied, ClientID, TenantID and ClientSecret, and SSL/TLS must be enabled.

Full information on configuring OAuth can be found in the separate "2025 - Setting up Azure to Send Email Using OAuth" document which can be accessed here: https://sites.riskman.net.au/RiskManDownloads/Documents/2025-Setting-up-Azure-to-Send-Email-Using-OAuth.pdf . Please contact RiskMan Support on **1800 018 984 (Outside Australia: +61 (0) 391 257 670)**, or via Customer Portal for information on configuring OAuth

Please Note: Due to the way modern mail servers provide information back to RiskMan, within the Email Log the "Date Sent" refers to the date the mail server accepted the email, this does not guarantee that the email is delivered to the user. For example, if an incorrect address has been entered in a user profile, it may show in the email log as sent, as the mail server accepted the email, even though it was never delivered as the email did not exist. RiskMan does not have the ability to manage emails once they have been accepted by the mail server, therefore cannot guarantee they will be received by the intended user, or that the user's email address is a valid email

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): Administration | Global Settings

Key: RMI-10926

Changed the image which appears on the RiskMan Error (pink screen) page so that it is a more contemporary image

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): System | Miscellaneous

Key: RMI-11310

Modified the QF_XML_Definitions table "Definition" column to be a datatype of XML for performance improvements, and all corresponding code updated to use this datatype

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): Performance | Code-related

Key: RMI-11249

Enhanced the attached document functionality by changing the document links so the dynamic Val request string is now 42 characters long and an encrypted value using both alphabetical and numeric values (previously it was 4 alphabetical characters) to add additional security to the documents.

This results in the possibility of guessing the correct Val going from a 26^4 (ie 456,976 combinations) to a possibility of 36^{42} (ie 2315821236788381026727364905671113865038583618100758591103261736 96 combinations)

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): Security | Code-related

Key: RMI-11344

Resolved a potential security issue on the Review History page accessible from grid listing to prevent any cross-site scripting from the Journal Description fields if they are populated with html or javascript information

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): Security | Code-related

Key: RMI-11345

Improved the security of HTTP headers within the system by adding some Content-Security-Policy (CSP) and Permissions-Policy Headers

Significance: ■ ■ ■ Need for training: ■ ■ ■

Module(s): Security | Code-related

Key: RMI-11346

Fixes

Resolved an issue with the styling of the header on the "Create New User Login" page to ensure it displays correctly

Module(s): System | Miscellaneous

Key: RMI-11291

Removed the obsolete wording on the iPad Welcome screen which referred to an audit table

Module(s): System | Miscellaneous

Key: RMI-11292

Resolved an issue with Draft where it could incorrectly show the "Autosave Found" screen if you immediately opened a record after saving a draft

Module(s): Performance | Code-related

Key: RMI-11278

Corrected error handling for Workbook Reports as it previously recorded blank error messages

Module(s): Analysis | Workbook Reports

Key: RMI-11314

Known Issues

No know issues reported