Workshare Risk Analytics 1.6

Release Notes

Table of Contents

What is Risk Analytics 3
What's new in this release 4
System Requirements 4
Hardware 4
Software 4
Prerequisites 5
Database user credentials 5
Upgrading 5
Known Issues 6
Contact Info 6

What is Risk Analytics

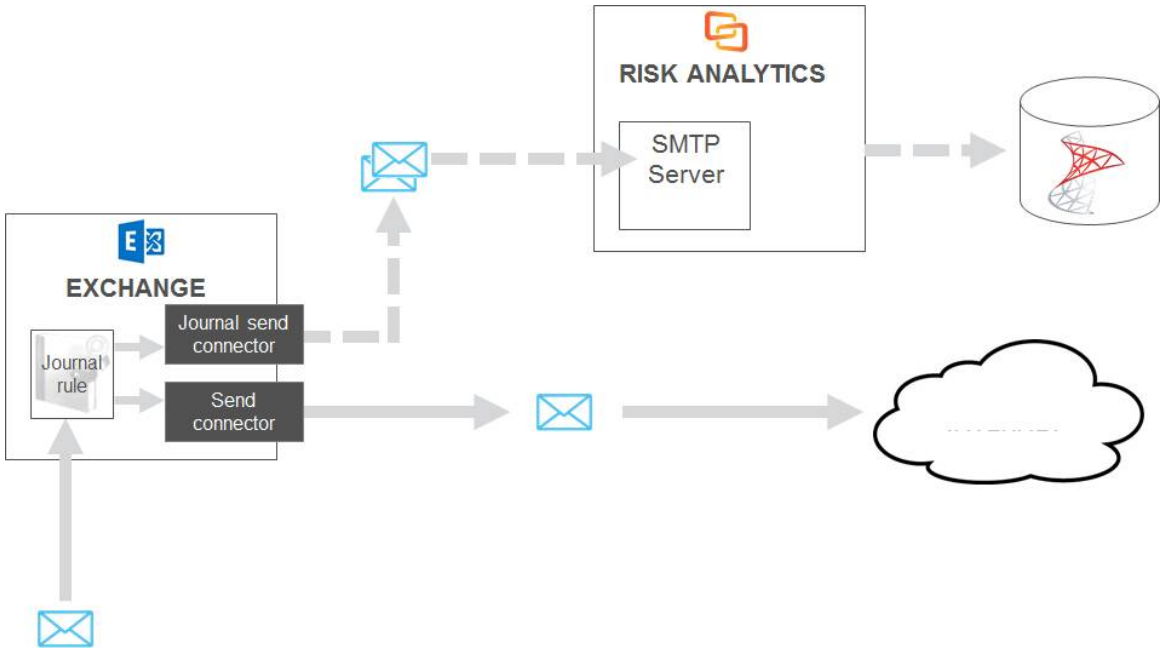
Workshare Risk Analytics enables compliance admins to monitor outgoing emails, giving them the information they need to analyze data security breaches. It does this by capturing a copy of all emails sent outside the company and storing information about every email and its attachments. Compliance admins can then run reports on the data so they can analyze the information and implement policy accordingly.

For example, Risk Analytics stores information about all custom properties found in an attachment. This could be custom properties automatically added by a DMS or manually added by a user. Compliance admins can trace all documents sent out that included a specific custom property and identify who sent that document.

Comprehensive filtering of this large amount of data enables compliance admins to identify a problem, get to the root of it quickly and, consequently, react to data breaches promptly.

Risk Analytics is adaptable and configurable tackling data protection without risk to email flow:

- Monitor emails, without blocking
- React quickly to discover the source of data leaks
- Check the email activity of departing employees
- Comply with data protection regulations



What's new in this release

The 1.6 release of Risk Analytics includes the free domains report. This report provides information on emails with attachments that are sent to email addresses with a non-corporate domain, such as hotmail.com or yahoo.co.uk.

System Requirements

Workshare Risk Analytics must be installed on its own dedicated server. The minimum specifications for the Risk Analytics machine are given below.

Hardware

Server class machine for Risk Analytics:

- 4 processing cores, 8GB RAM, 120GB HDD space

(optional) Server class machine for data aggregation and business intelligence:

- 4 processing cores, 16GB RAM, 250GB HDD space

(optional) Server class machine for document tagging:

- 2 processing cores, 4GB RAM, 120GB HDD space

Software

Server for Risk Analytics:

- Operating system: Microsoft Windows Server 2016 or 2012 R2
- Microsoft Exchange Server 2016 or 2013
- Microsoft SQL Server 2012 and above (2014 is recommended)

(optional) Server for data aggregation and business intelligence:

- Operating system: Microsoft Windows Server 2016 or 2012 R2
- Anaconda and Python 3.x
- Tableau (optional, for business intelligence)

(optional) Server for document tagging:

- Operating system: Microsoft Windows Server 2012 R2 Standard/Datacenter x64 Edition
- Worksmart DLPTagger from HBR Consulting

Prerequisites

The following software must be installed prior to the installation of Workshare Risk Analytics.

- Microsoft .NET Framework 4.5.2
- Microsoft Internet Explorer 11+

In addition, ports 80 and 443 must be open for web traffic on the Risk Analytics server.

Risk Analytics requires certain Windows features to be enabled. This is described as part of the deployment process in the Installation Guide.

Database user credentials

The following users are required:

- **Database administrator**: The credentials for this user must be available prior to installation. The database administrator can be an SQL user or a Windows domain user, as long as they have a sysadmin role (or enough rights to create databases and assign users to databases). The database administrator user is required during installation to create database tables and to set up the processor user. These credentials are not stored after installation.
- **Risk Analytics processor user**: If using Windows authentication, the credentials for this user must be available prior to installation. If using SQL authentication, the installer will create a user (with database read and write permissions to the Risk Analytics database) if one doesn't exist. The processor user should have a "public" role only and cannot be the same user as the database administrator. This user is to enable communication between Risk Analytics and the database and would typically only be given minimum access permissions (to the Risk Analytics database catalog only). These credentials are stored on the Risk Analytics machine.

Upgrading

Workshare Risk Analytics does not support upgrades from earlier versions. You must uninstall previous versions and then install the Risk Analytics 1.6 software. Databases will be migrated automatically.

Known Issues

The following are known issues in the Workshare Risk Analytics 1.4 release - for more information, please contact Customer Support.

Ref	Description
RA-210	The **Anomalous Emails** section of the anomalies report loads more slowly than other sections.
RA-242	Unable to re-access the admin registration URL (https://localhost/risk-analytics/Wizard/PostInstall) if a user closes the browser after clicking the **Launch Risk Analytics** button.
RA-370	Cannot install using Windows Authentication when domains contain special characters.
RA-593	If Risk Analytics is un-installed and then re-installed with a different database name, the installation will fail.
RA-773	Unprocessed emails are not saved in the unprocessable email save location after installing the Feedback service plug in and stopping and restarting the SQL service.
RA-808	A non-logged in user can call the reports/free-domains API.
RA-828	A 500 status code is returned when the applied date filter is in an invalid format.

Contact Info

For technical help and support on Workshare products, contact Workshare Customer Support:

support@workshare.com
EMEA: +44 207 539 1400
US: +1 415 590 7705

For sales enquiries, contact the Workshare Sales team:

sales@workshare.com
EMEA: +44 207 426 0000
US: +1 415 590 7700
APAC: +61 2 8220 8090

Workshare Ltd.
© 2019. Workshare Ltd. All rights reserved.

Copyright
Workshare Professional and Workshare DeltaView are registered trademarks of Workshare Ltd. Workshare Compare, Workshare Protect, Workshare 3, Workshare DeltaServer, SafetyGain, and the Workshare logo are trademarks of Workshare Ltd. All other trademarks are those of their respective holders.

Trademarked names may appear throughout this guide. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

Disclaimer
The authors/publishers of this guide and any associated help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective help material possible.

The authors/publishers, however, make no warranty of any kind, expressed or implied, with regard to Workshare programs or help material associated with them, including this guide. The authors/publishers shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the programs or associated help instructions.

For details of Workshare patents, see www.workshare.com/patents

Revisions
Published for Workshare Risk Analytics 1.1: 01/02/18
Revised for Workshare Risk Analytics 1.3: 15/05/18
Revised for Workshare Risk Analytics 1.4: 20/07/18
Revised for Workshare Risk Analytics 1.6: 31/01/19

Workshare Ltd., 20 Fashion Street, London E1 6PX www.workshare.com