Workshare Risk Analytics

Installation Guide

Table of Contents

Chapter 1: Introduction....3
What is Risk Analytics....4
System Requirements....5
Hardware....5
Software....5
Prerequisites....5
Environment....6
Database user credentials....6
Chapter 2: Deployment....7
Installation Files....7
Upgrading....7
Deploying Risk Analytics....7
Step 1: Install prerequisites....8
Windows prerequisites....8
Runtime prerequisites....10
Step 2: Configure SMTP server....10
Step 3: Install Risk Analytics software....19
Step 4: Configure Exchange....26
Step 5: License and test the Risk Analytics deployment....27
(optional) Step 6: Custom property stamping on documents....29
(optional) Step 7: Business intelligence reporting....29
Chapter 3: Configuration....30
Inviting Users....30
What the invited user sees....31
Command utility to add users....32
Domain Classification....33
Selecting Emails to Monitor....34
Protect Server configuration....35
Content extraction....36

Chapter 1: Introduction

This chapter introduces Workshare Risk Analytics, providing an overview of how it works and the system requirements for installation. It includes the following sections:

- **What is Risk Analytics?**, page 4, introduces Workshare Risk Analytics.
- **System Requirements**, page 5, describes the requirements for installation.

What is Risk Analytics

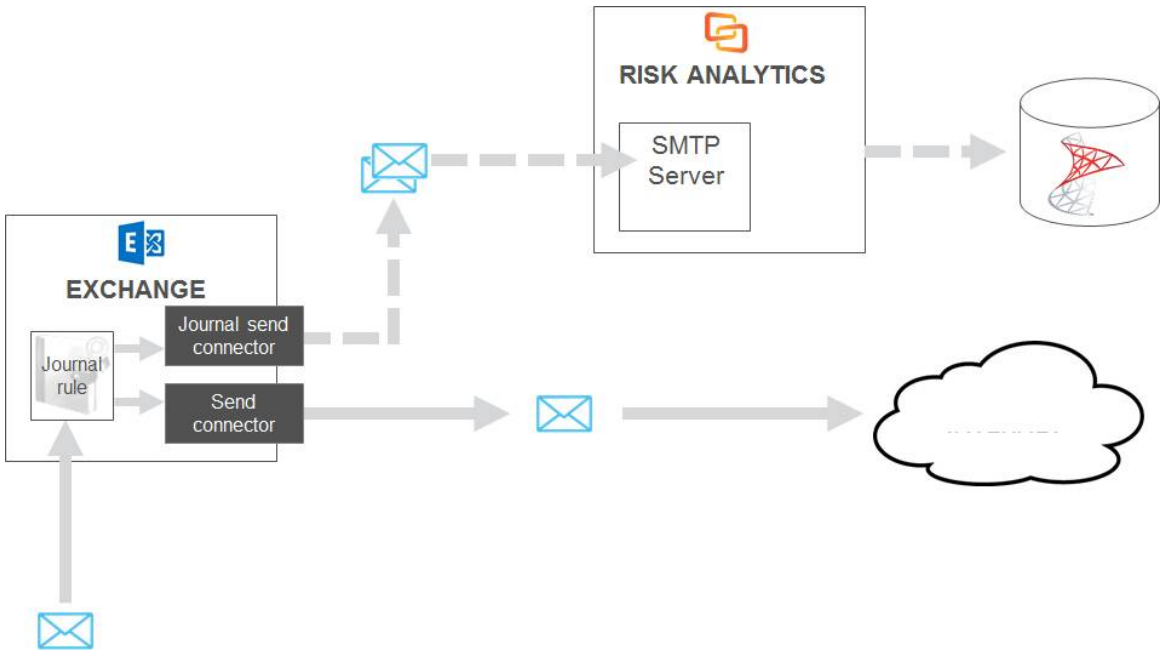
Workshare Risk Analytics enables compliance admins to monitor outgoing emails, giving them the information they need to analyze data security breaches. It does this by capturing a copy of all emails sent outside the company and storing information about every email and its attachments. Compliance admins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



System Requirements

The minimum specifications for the Workshare 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

(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 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 Step 1: Install Windows prerequisites.

Environment

In your Risk Analytics environment, Microsoft Exchange Server is required as well as a database with Microsoft SQL Server. SQL Server 2014 is recommended but Risk Analytics works with SQL Server 2012 and above.

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.

Chapter 2: Deployment

This chapter describes how to deploy and set up Workshare Risk Analytics in your environment. It includes the following sections:

- **Installation Files**, page 7, describes the files included in the Risk Analytics installation bundle.
- **Deploying Risk Analytics**, page 7, describes each step of the deployment process.

Installation Files

The following files are included in your Workshare Risk Analytics installation bundle:

- risk-analytics-installer- [version number].exe
- install-ra-prerequisites-win2012.ps1
- deployment-test.msg (this is a test file to use during validation of the installation)

You should save these files locally. For the installation described in this guide, the files have been saved to C:\RAInstall.

***Note**: You will also receive a LIC file to license Risk Analytics.*

On your Risk Analytics machine, you install the Windows prerequisites, configure SMTP server and then install the Risk Analytics executable. You will also have to perform some configuration on Exchange.

Upgrading

Risk Analytics does not support upgrades from earlier versions. You must uninstall previous versions and then repeat step 3 below to install Risk Analytics 1.3. Databases will be migrated automatically.

Deploying Risk Analytics

The installation and setup of Workshare Risk Analytics includes the following steps:

Step 1: Install Windows prerequisites

Step 2: Configure SMTP server

Step 3: Install Risk Analytics software

Step 4: Configure Exchange

Step 5: License and test the Risk Analytics deployment

(optional) Step 6: Custom property stamping on documents

(optional) Step 7: Business intelligence reporting

Follow these steps in the order shown.

Step 1: Install prerequisites

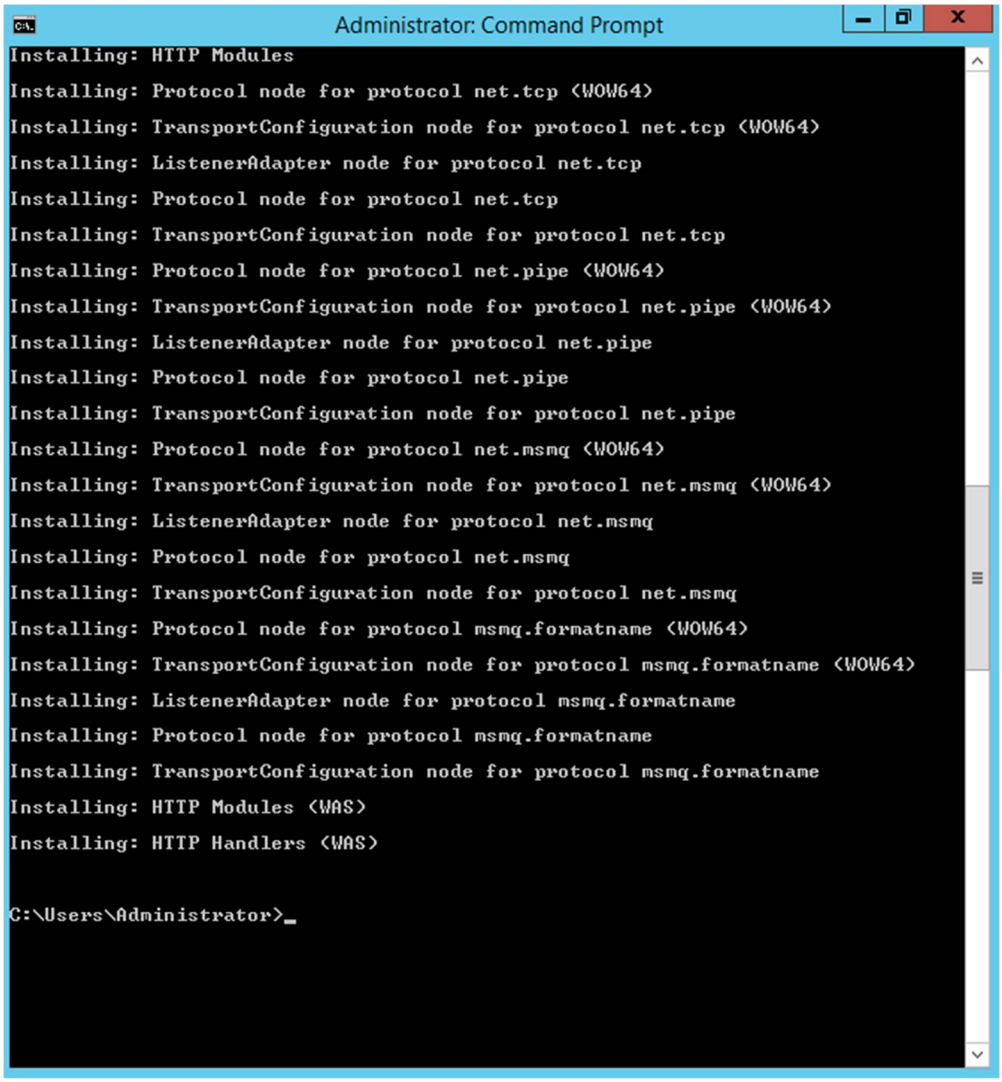
Windows prerequisites

A PowerShell script (**install-ra-prerequisites-win2012.ps1**) is included with the installation to add the Windows features required for Risk Analytics.

To install the Windows prerequisites:

1. On your Risk Analytics machine, open a command prompt as administrator.
2. Type: `@powershell -ExecutionPolicy Bypass -Command "C:\rainstall\install-ra-prerequisites-win2012.ps1"`

3. Press Enter on your keyboard. This command checks permissions and runs the PowerShell file to install the required Windows features. Once complete, you will see:



***Note**: If there is a "the source files could not be found/downloaded" error, run the procedure described here: https://technet.microsoft.com/en-GB/library/dn482071.aspx*

Runtime prerequisites

The following three redistributable packages need to be installed before installation of Risk Analytics:

- **Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL Security Update**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/6/B/B/6BB661D6-A8AE-4819-B79F-236472F6070C/vcredist_x86.exe

- **Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package ATL Security Update**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/9/7/7/977B481A-7BA6-4E30-AC40-ED51EB2028F2/vcredist_x86.exe

- **IIS URL Rewrite**

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/6/7/D/67D80164-7DD0-48AF-86E3-DE7A182D6815/rewrite_2.0_rtw_x64.msi

Step 2: Configure SMTP server

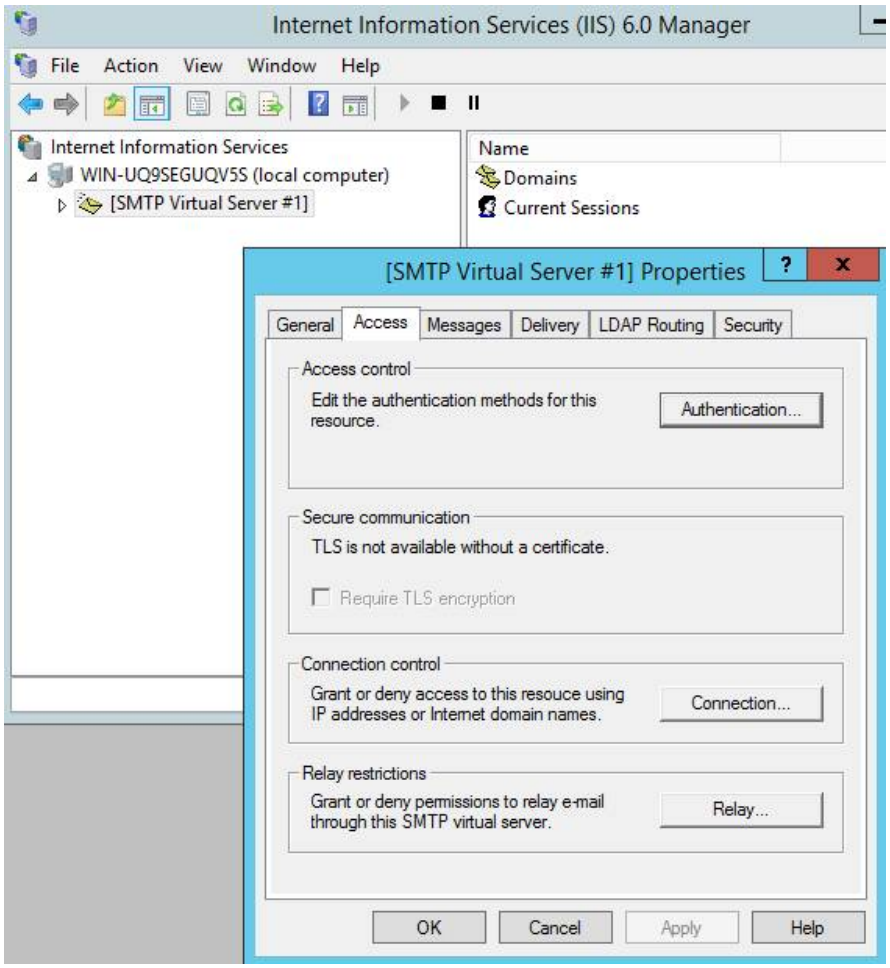
The SMTP server on the Risk Analytics machine receives the journaled email (copies of emails) from Exchange Server. This step is to configure the SMTP server to accept emails from your exchange environment.

By default, Risk Analytics consumes emails that have been processed so the SMTP server will not relay them on for delivery. However, as added security to ensure emails are not relayed unintentionally, this step also configures SMTP server to accept emails and not relay them further.

In order to configure the SMTP server, you need to decide on the journaling email address. This should be unique for your organization. For the installation described in this guide, the journaling email address used is **journal@riskanalytics.local**.

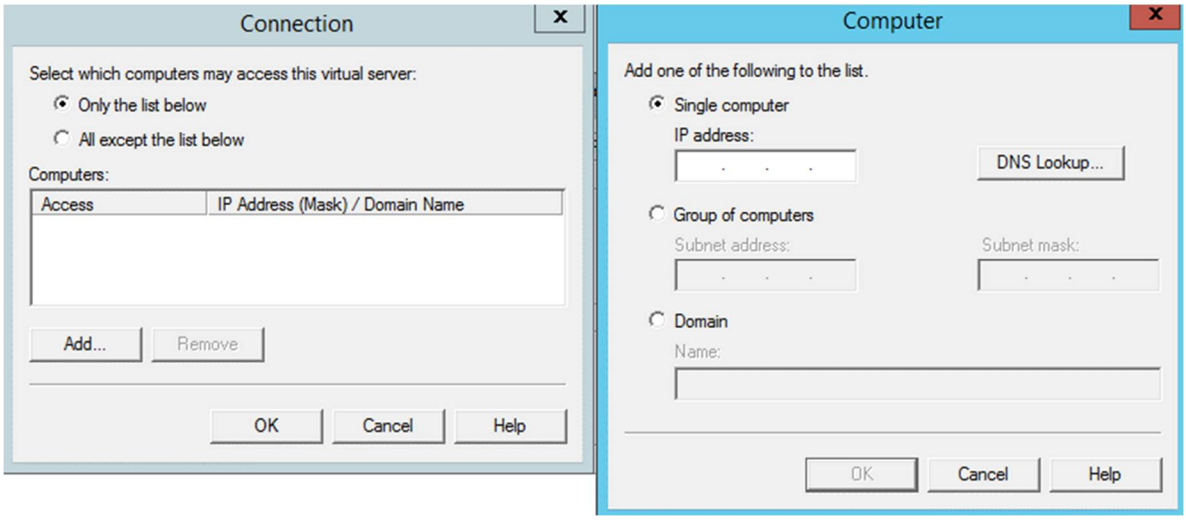
To configure the SMTP server:

1. On your Risk Analytics machine, open Internet Information Services (IIS) 6.0 Manager.
2. Open SMTP server properties.
   - Expand the local computer.
   - Right-click **[SMTP Virtual Server #1]** and select **Properties**.

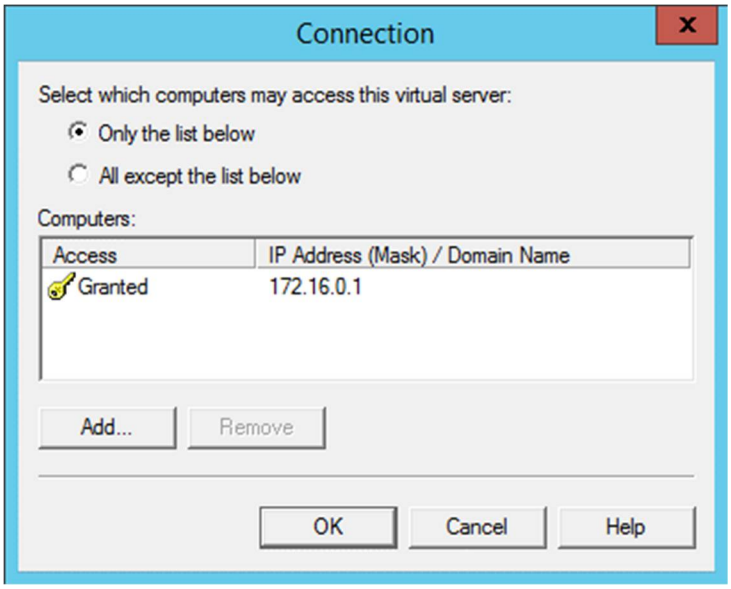


3. Select the **Access** tab.

4. Add a connection rule to allow Exchange servers to connect to the SMTP server on the Risk Analytics machine.
   - In the **Connection control** area, click **Connection**.
   - Select **Only the list below**.
   - Click **Add**.



   - Select **Single computer**.
   - Enter the IP address of your Exchange server.
   - Click **OK**.



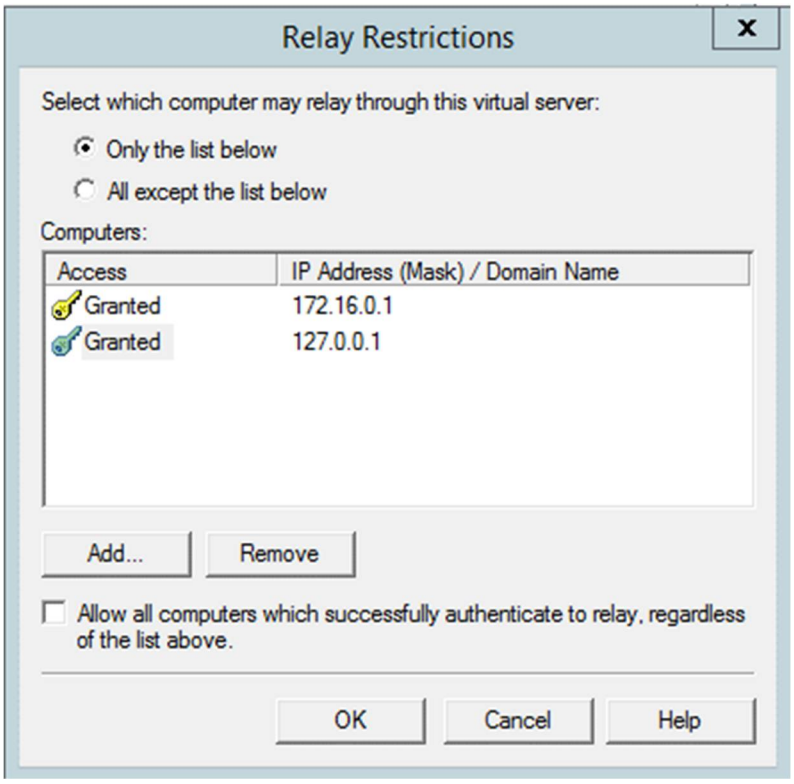
***Note**: Repeat this process if you have more than one Exchange server so you have the IP addresses of all of them listed in the Connection dialog.*

   - Click **OK**.

5. Add a relay rule to allow Exchange servers to relay to the SMTP server on the Risk Analytics machine.
   - In the **Relay restrictions** area, click **Relay**.
   - Select **Only the list below**.
   - Click **Add**.
   - Select **Single computer**.
   - Enter the IP address of your Exchange server.
   - Click **OK**.

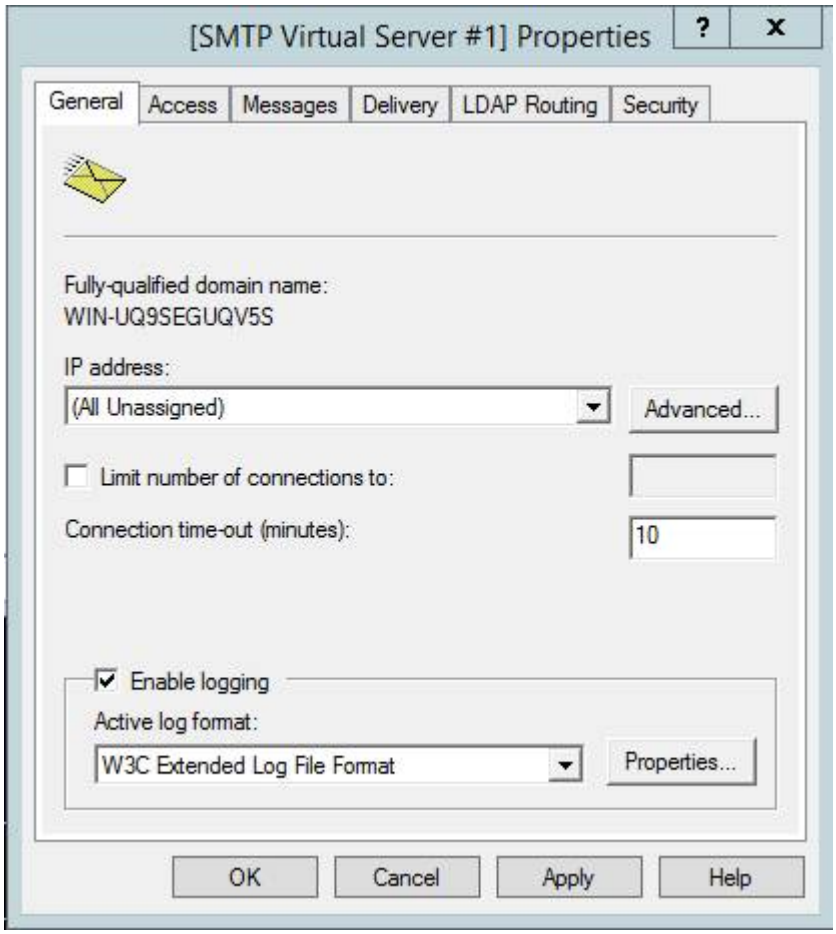
> ***Note**: Repeat this process if you have more than one Exchange server so you have the IP addresses of all of them listed in the Connection dialog.*

   - Click **Add**.
   - Select **Single computer**.
   - Enter the IP address 127.0.0.1 to ensure that Risk Analytics can send password reset emails.
   - Click **OK**.



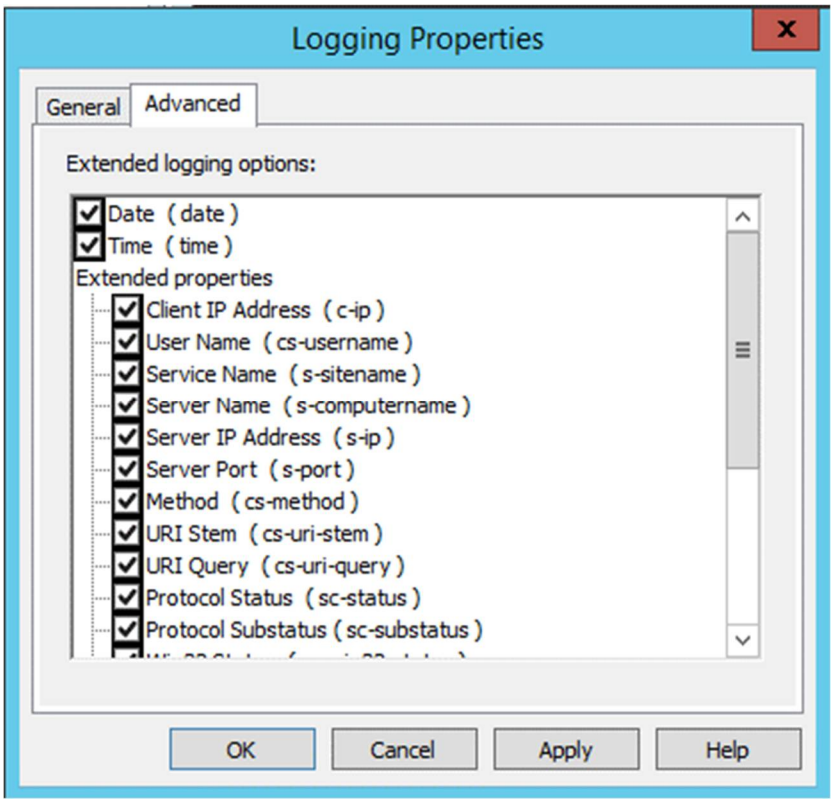
6. Click **OK** in the Relay Restrictions dialog.
7. Select the **Messages** tab.
8. Set the message size parameters to match your organizational limit.

9. Select the **General** tab.



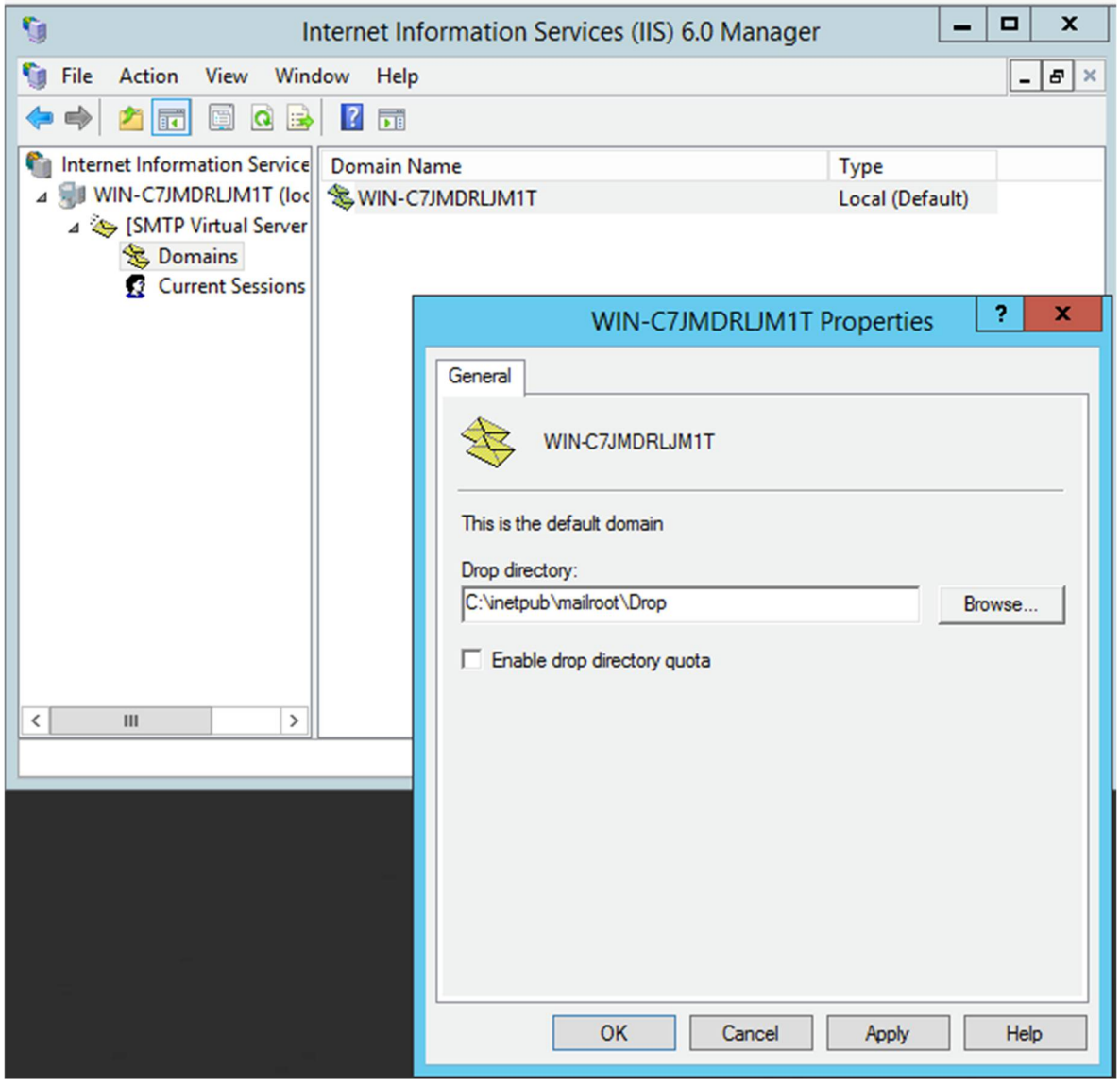
10. Select **Enable logging** and click **Properties**.

11. Click **Advanced** and select all of the extended properties.



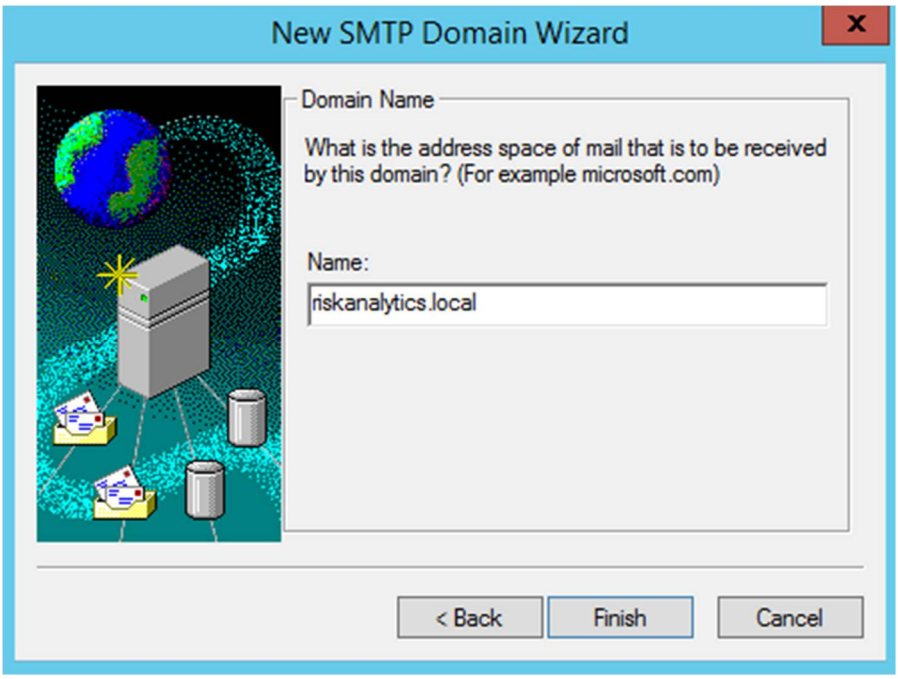
12. Click **OK**.
13. Click **OK** in the Properties dialog.
14. Right-click the **Local (default)** domain, and select **Properties**.

15. Ensure that the **Enable drop directory quota** checkbox is NOT selected.

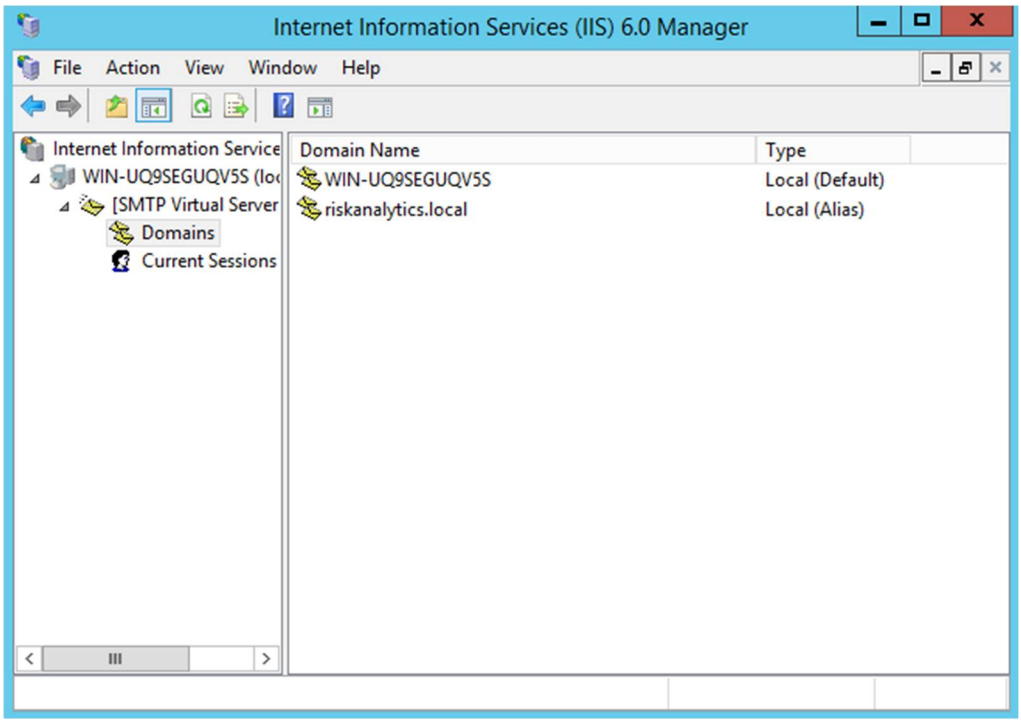


16. Click **OK**.

17. Set up a new SMTP domain with the domain of your journaling email address.
    - Right-click in the blank space on the right and click **New > Domain**.
    - Select **Alias** as the domain type.
    - Click **Next**.
    - Enter the domain name of your journaling email.



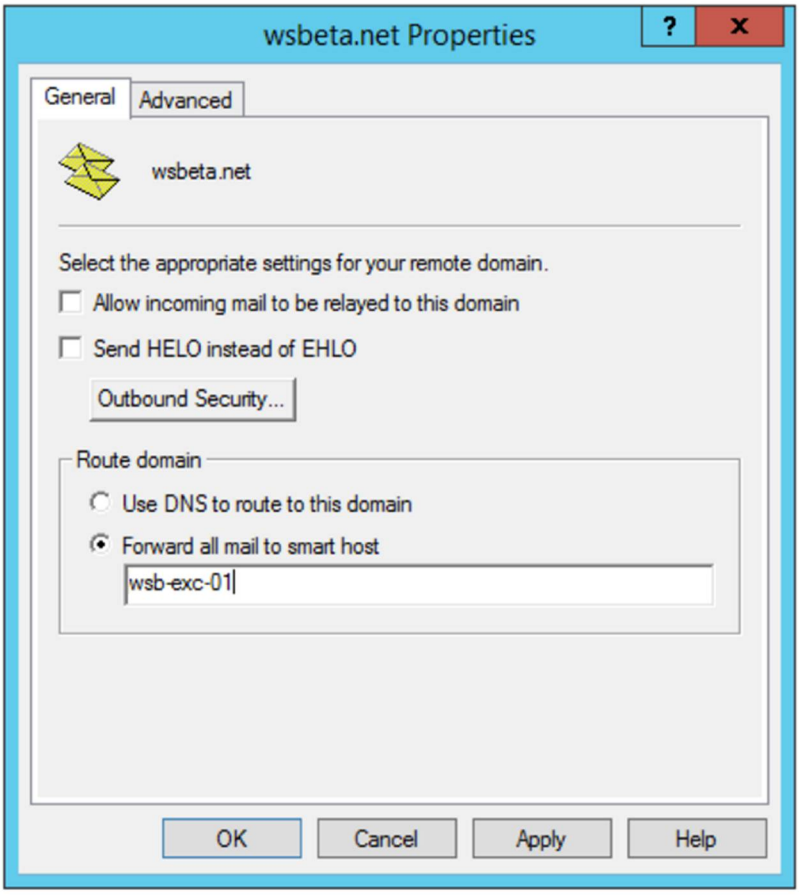
    - Click **Finish**.



18. Create a route for user management email back to your Exchange server.
    - Right-click in the blank space on the right and click **New** > **Domain**.
    - Select **Remote** as the domain type.
    - Enter the email domain used by the email addresses of the administrators of Risk Analytics.

> ***Note**: If there is more than one email domain to manage, then these need to be configured in the same manner.*

    - Once the domain has been created (wsbeta.net as an example), right-click and select **Properties**.



    - In the **Route domain** section of the **General** tab, select **Forward all mail to smart host**. Enter the address of the Exchange server that the email for that email domain is to be delivered to (wsb-exc-01 as an example).

Step 3: Install Risk Analytics software

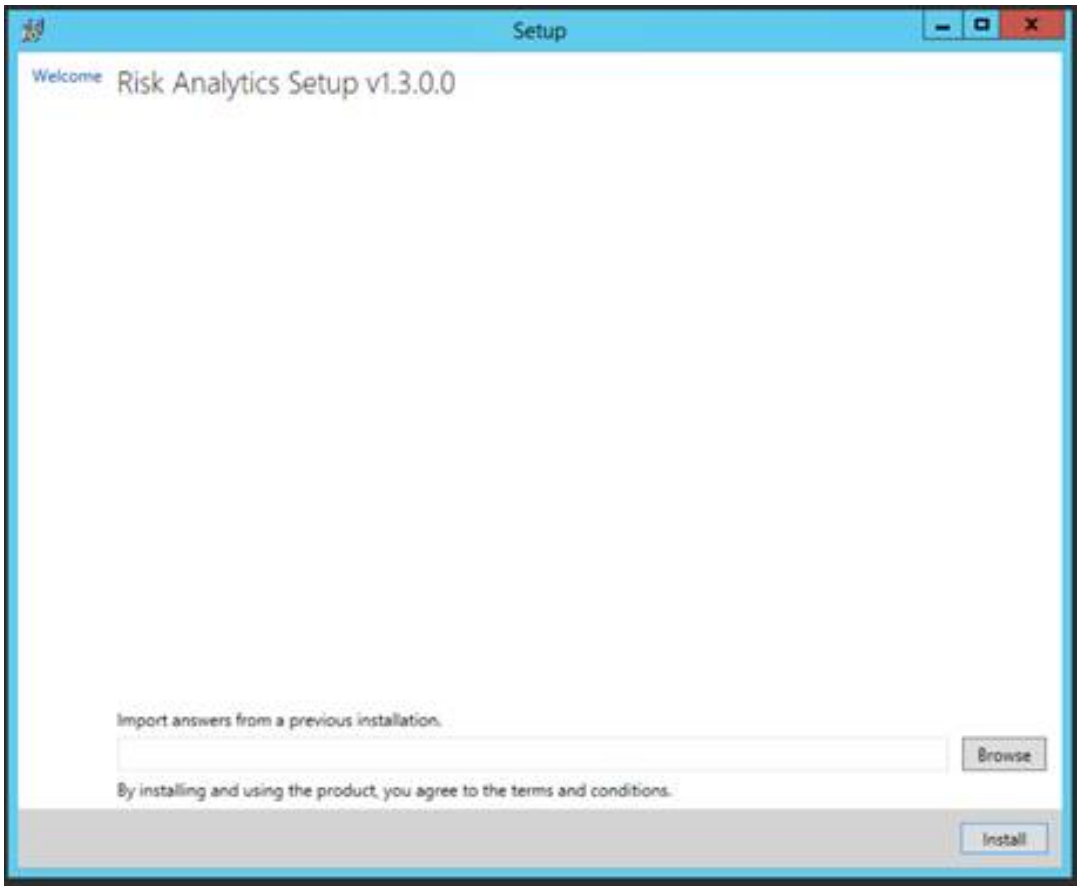
In this step, you run the Risk Analytics executable. During the installation, you will be prompted to enter:

- Database details.
- API keys. These secure the REST API that is used by the Mail Transport Agent (MTA) and potentially other future web services.
- A location to save unprocessable emails.

This step in the installation process normally takes between 2 to 5 minutes.

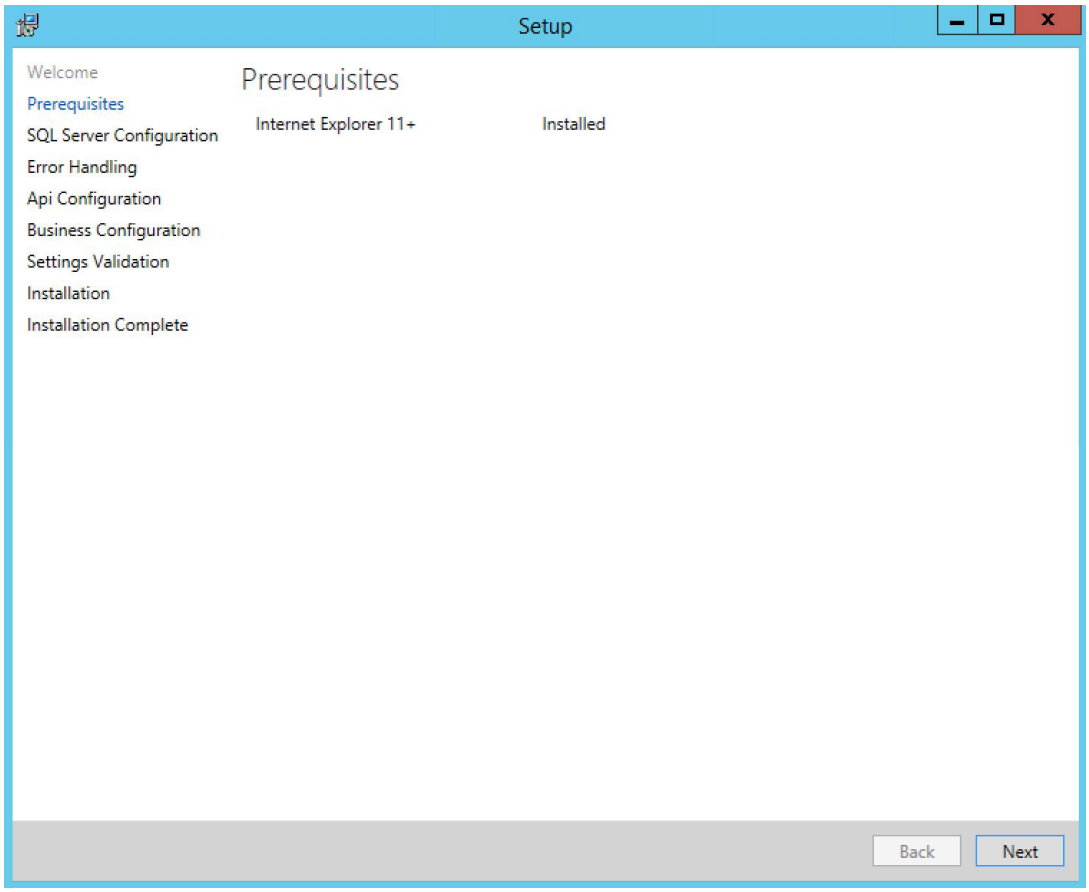
To install the Risk Analytics software:

1. On your Risk Analytics machine, run the Risk Analytics executable.

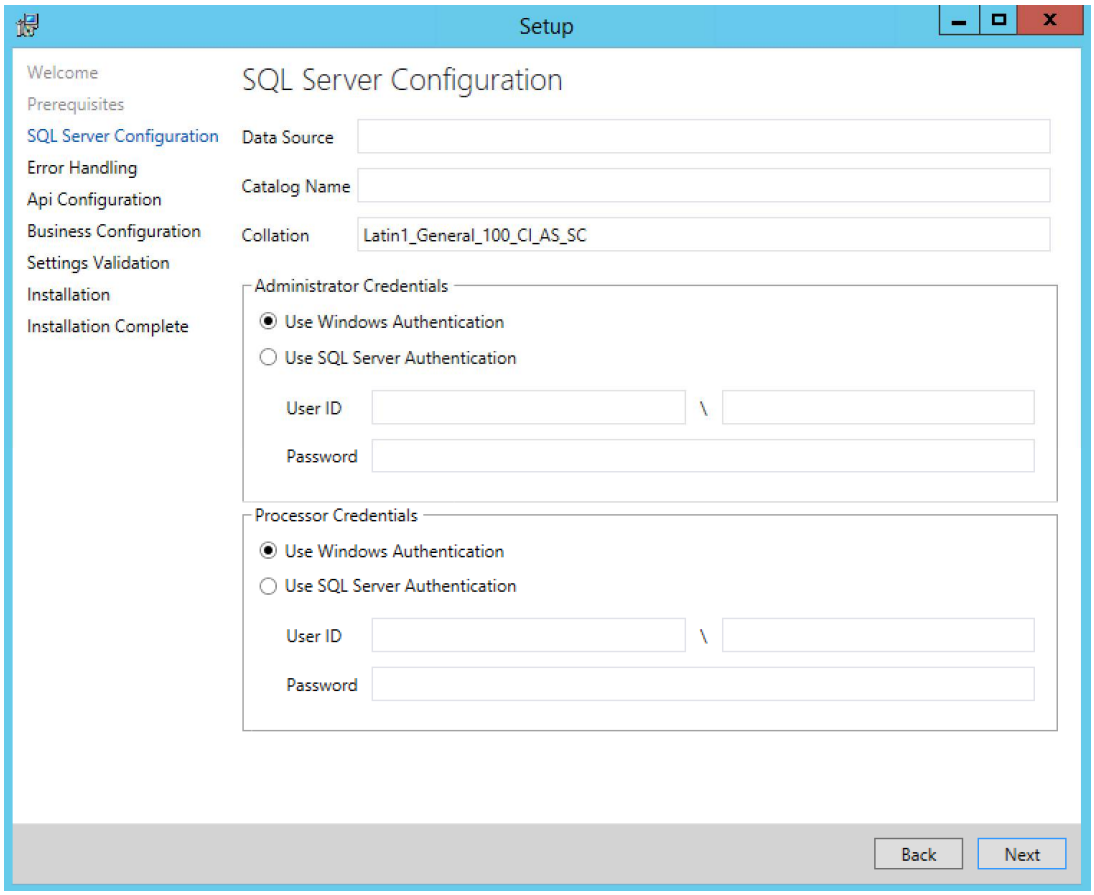


***Note**: Every installation creates an answer file that can be re-used in subsequent installations. You may provide an answer file containing previously entered configuration if available and applicable. You will need to re-enter passwords.*

2. Click **Install**. The Prerequisites page is shown confirming whether the prerequisites are installed.

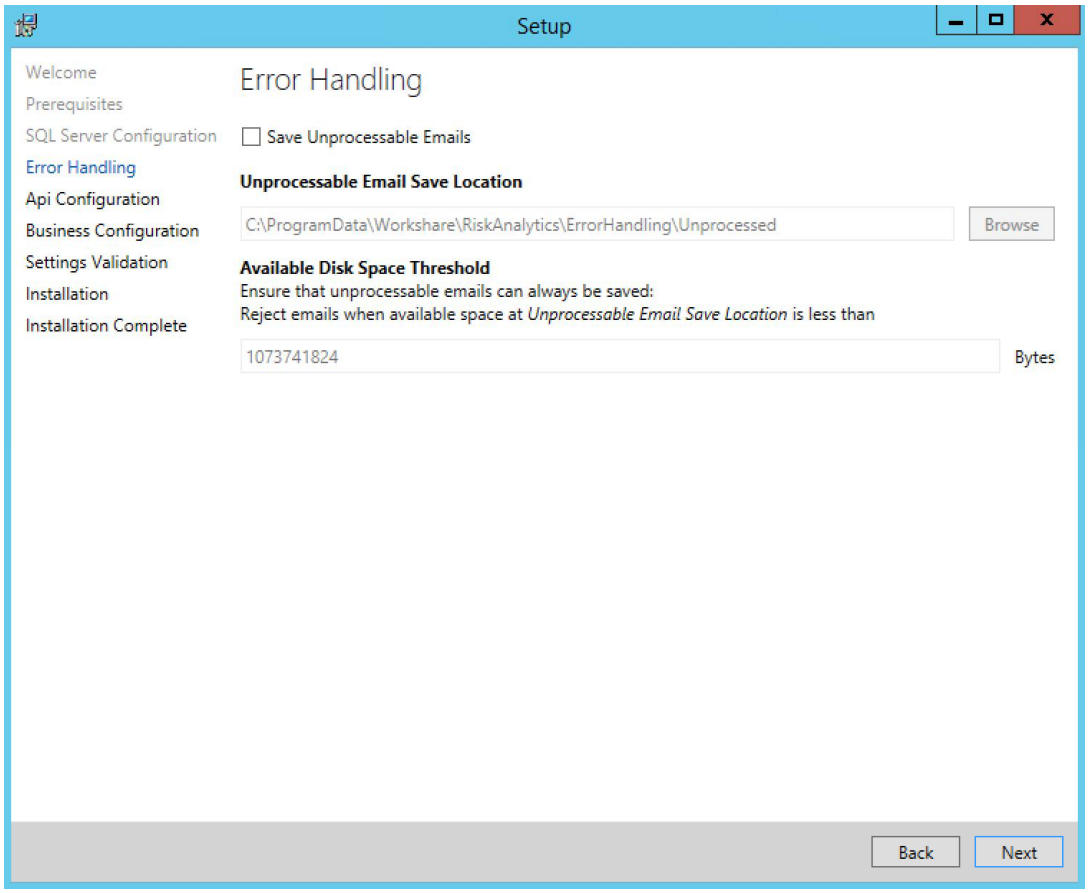


3. Click **Next**.



4. In the **Data Source** field, enter the location of your database. This is the IP address or host name of your SQL server.
5. In the **Catalog Name** field, enter a name for your Risk Analytics catalog in your database, for example, RADB.
6. The **Collation** controls the rules by which strings are sorted by in the database so you might need a different collation when using a foreign language. The default collation for Risk Analytics should be good for western European countries. If your SQL administrator has configured a default collation for the SQL server, you should leave this field blank.
7. In the **Administrator Credentials** area, enter the details for your administrator user (described in Database user credentials).
8. In the **Processor Credentials** area, enter the details for your processor user. If you select **Use SQL Server Authentication**, the user will be created if the user doesn't already exist.

9. Click **Next**.

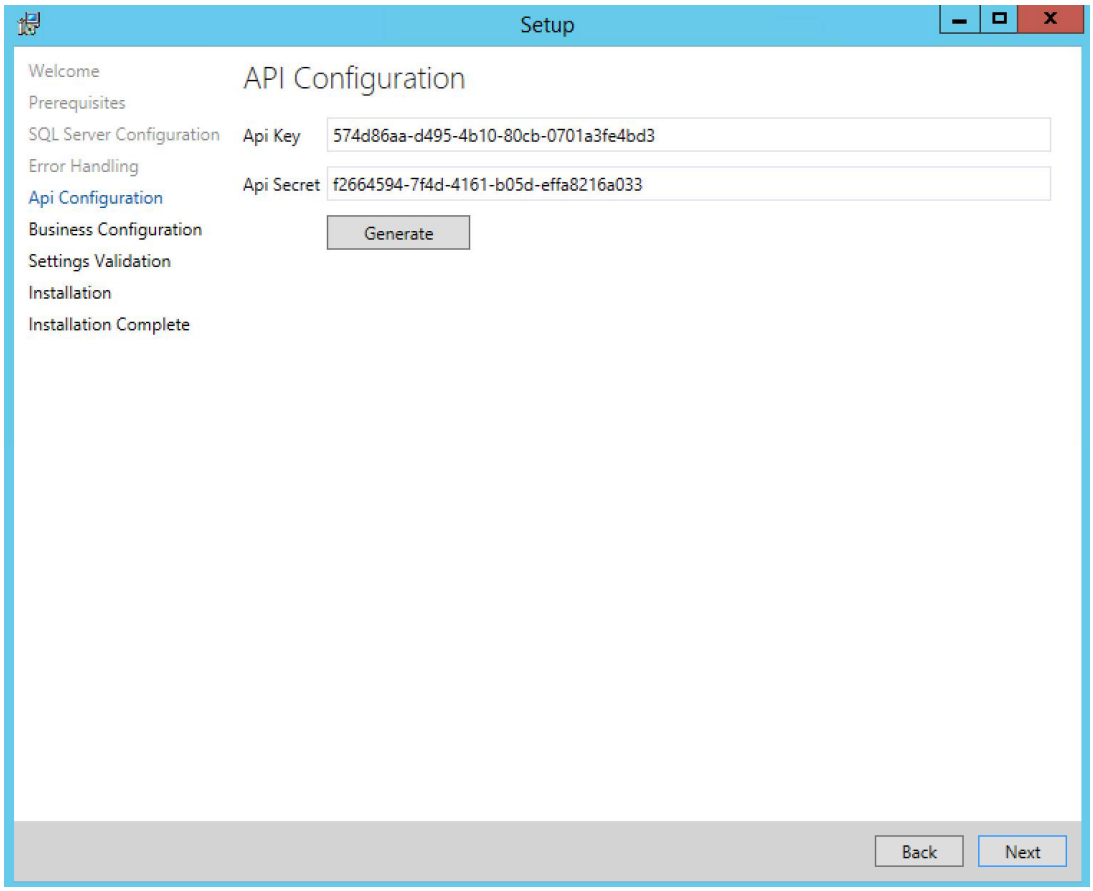


10. Select **Save Unprocessable Emails**. This means that if there are email journals that Risk Analytics cannot process, it will save them in the location shown. Click **Browse** and change the location if required.

11. Leave the **Available Disk Space Threshold** as the default of 1073741824 bytes (1 gigabyte). This means that if there is less than 1 gigabyte of space in the **Unprocessable Email Save Location**, Risk Analytics will reject the email journal and it will sit in a queue in Exchange waiting.

> ***Note**: Exchange will route the email journal to another Risk Analytics machine if one is configured.*

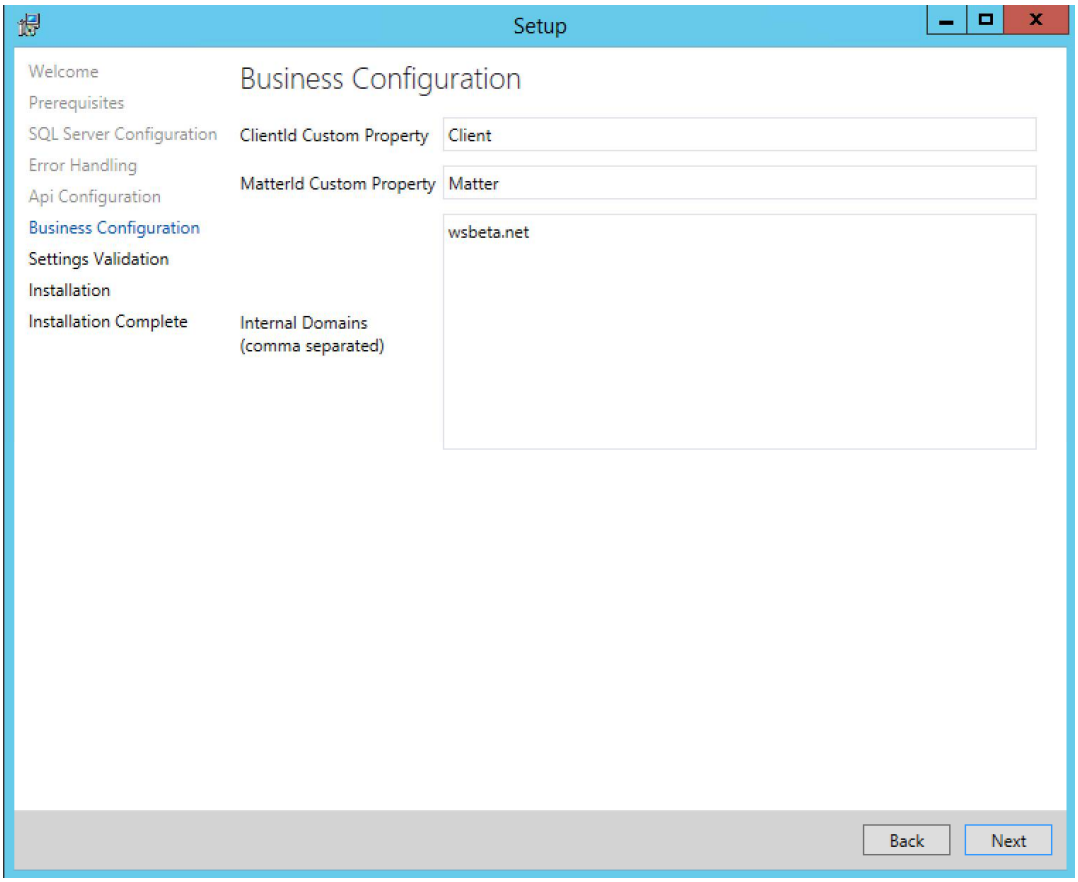
12. Click **Next**.



13. In the API Configuration page, click **Generate** to generate a random set of keys that will secure access to the Risk Analytics API.

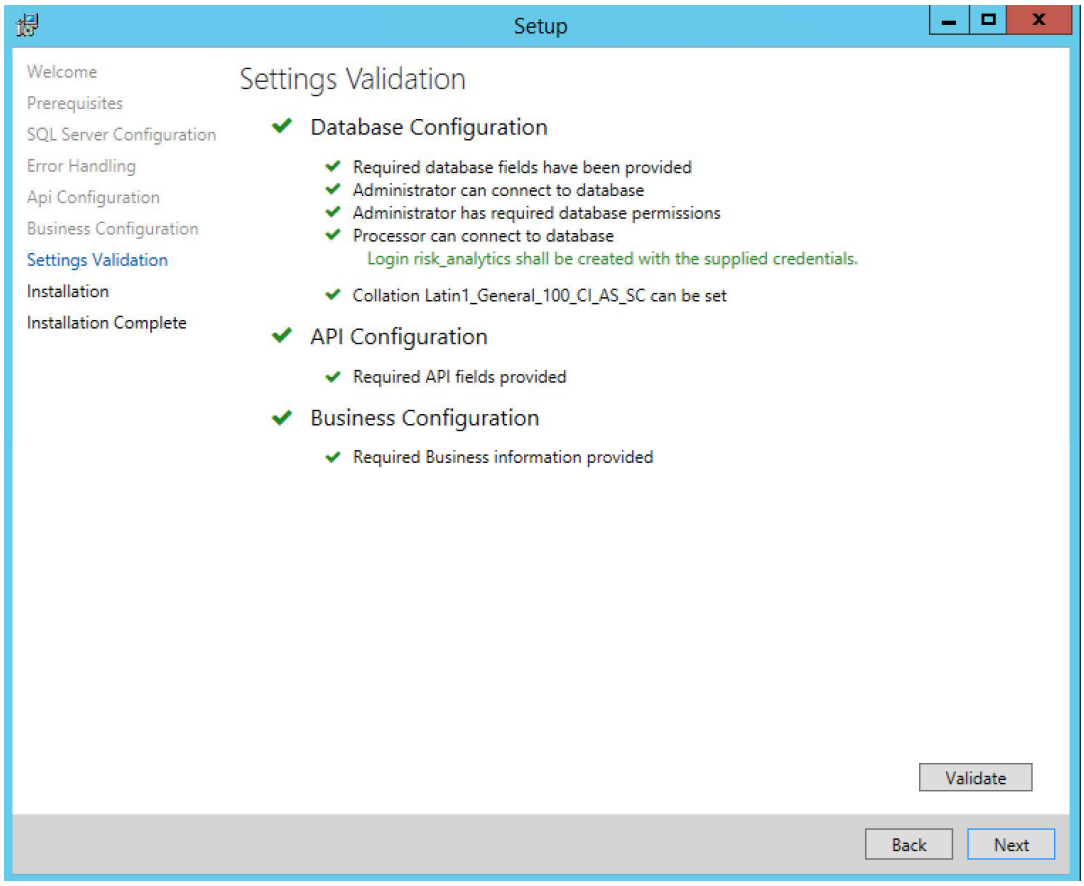
> ***Note**: If you are installing multiple instances of Risk Analytics, the same API key and secret should be used for each one.*

14. Click **Next**.



15. In the **ClientId Custom Property** and **MatterId Custom Property** fields, enter the custom property (key) you use to identify clients and matters. Risk Analytics will monitor these keys and record their values.
16. .In the **Internal Domains** field, enter your internal domains so that Risk Analytics can identify which emails are going to internal recipients.
17. Click **Next**.

18. In the Settings Validation page, click **Validate**.



19. Click **Next**. Risk Analytics is installed. This process may take several minutes.
20. Once the installation is complete, click **Next**.
21. Click **Launch Risk Analytics**. Your browser opens showing the login page.

22. Enter your name, organization and email, and set a password. You will be an administrator user for Risk Analytics.
23. Click **Register**. The Risk Analytics console is displayed.

Step 4: Configure Exchange

On Exchange, you must create a send connector and a journal rule so that copies (journals) of all emails are sent to Risk Analytics.

- Add a send connector for Risk Analytics with the following details:
  - Address space: <your .local journal domain>
  - Smart host: [IP address or FQDN of Risk Analytics machine]
- Add a journal rule as follows:
  - Journal outbound email to <your journal address>
- Add a receive connector for administrators and users to receive user management emails and custom reports.

The procedure to add a send connector may vary according to your Exchange version. The following procedures describe how to create a send connector and a journal rule from the command line which is the same on all versions of Exchange.

To create a send connector:

1. Open Exchange PowerShell (also known as the Exchange Management Shell.
2. Enter the following command:

```
new-sendconnector -custom -name "Risk Analytics" -AddressSpaces
riskanalytics.local -SmartHosts "[<your risk analytics ip
address>]"
```

This creates a basic send connector. You may also need to modify your send connector for authentication, message size limits, additional smart hosts, etc. Refer to your Exchange administrator.

To create a new journal rule:

1. Open Exchange PowerShell (also known as the Exchange Management Shell.
2. Enter the following command:

```
new-journalrule -journalemailaddress journal@riskanalytics.local -
name "Risk Analytics" -Scope External -Enable $true
```

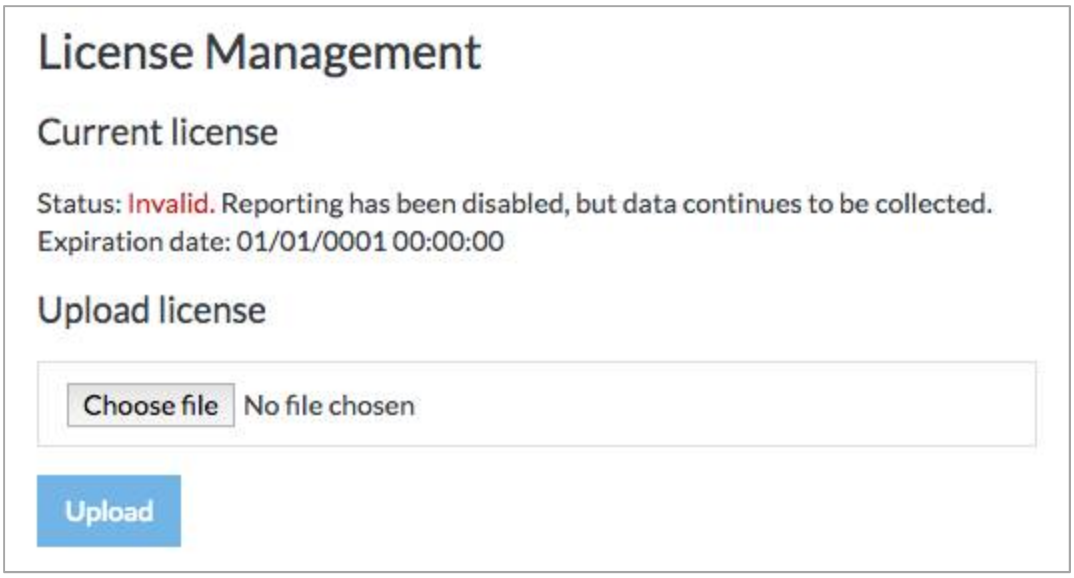
***Note**: You can limit journaling to a specific set of senders.*

Step 5: License and test the Risk Analytics deployment

You will need the LIC file provided by Workshare to license Risk Analytics.

To license Risk Analytics:

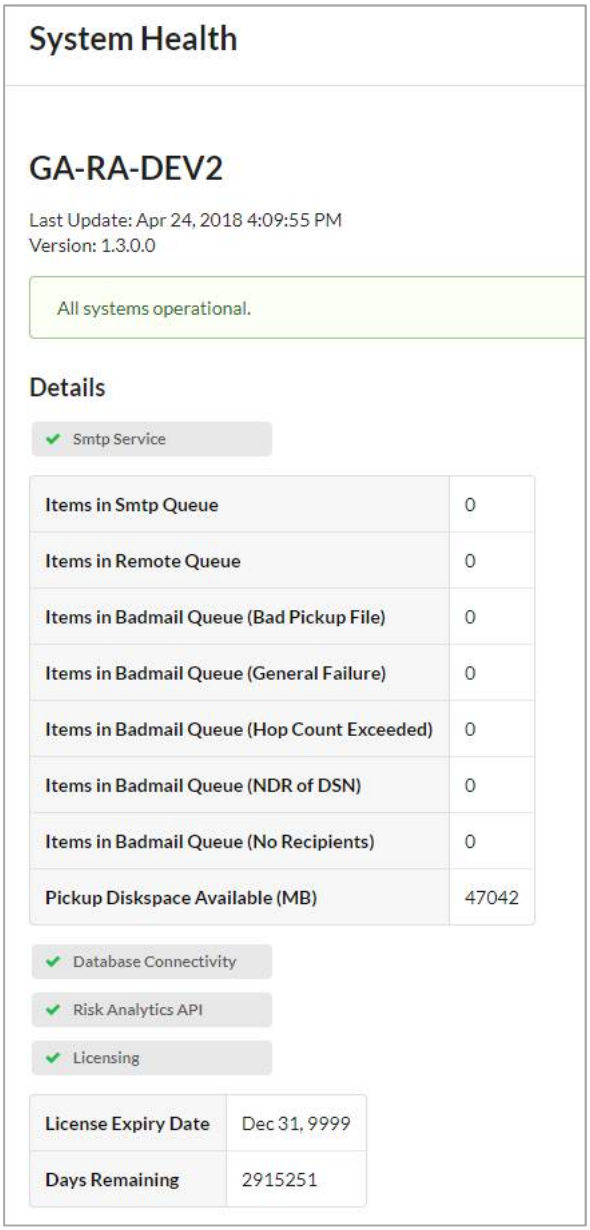
1. Log into the Risk Analytics console, select **Settings** and then **Licensing**.



2. Click **Choose File** and browse to the saved LIC file provided by Workshare.
3. Click **Upload**.

You can check your deployment was successful by following the steps below.

1. Log into the Risk Analytics console, select **System Health** and watch for all the lights to go green.



2. Use Outlook to send an email with the provided “deployment-test.msg” attached.
3. In the Risk Analytics console, select **Messages**.
4. Search for the top 20 email results where Custompropertyname equals **test-property** and Custompropertyvalue equals **workshare-test-id**.
5. You should see a single email result appear.

(optional) Step 6: Custom property stamping on documents

Risk Analytics uses custom properties within email attachments to identify documents and understand policy violation. These custom properties can be inserted manually, using template macros, or using a server-side tool. With manual and template macros, end-user training is required; with the server-side tool, no end-user workflows are affected.

A recommended server-side tool is the Worksmart DLPTagger tool from HBR Consulting for iManage installations. This tool is installed either co-located on the iManage server, or on a separate machine. The DLPTagger tool watches for save or re-index operations, and then tags documents within workspaces of interest with a pre-configured set of workspace properties.

The steps for installing the Worksmart DLPTagger tool are explained in detail in the DLPTagger Admin Guide. The prerequisites for the tool are:

- **Software:**
  - Operating system: Windows 7 or above
  - iManage: Version 8.5 or above
- **Access prerequisites:**
  - The DLPTagger service needs read access to the iManage DB catalog, and write access to its own DB catalog
  - The installation requires an Administrator-level (on the machine) service account that the DLPTagger service will run as. This service account needs to be able to access the iManage DB catalog (read-only) and the DLPTagger DB catalog (read-write)

(optional) Step 7: Business intelligence reporting

Risk Analytics reports anomalies and risk up to a business intelligence layer. This could be an in-house business intelligence system. If there is no in-house business intelligence system, Workshare can provide you with a Tableau Server installation. This software is licensed separately and directly from Tableau software.

Chapter 3: Configuration

This chapter describes how to configure settings for Workshare Risk Analytics in the Settings area of the console. It includes the following sections:

- **Inviting Users**, page 30, describes how to provide other users with access to the Risk Analytics console.
- **Domain Classification**, page 33, describes how to classify email domains in order to run queries against a particular email domain.
- **Selecting Emails to Monitor**, page 34, describes how to configure Risk Analytics to process only the email of selected senders.

Inviting Users

The first person that logs in to Workshare Risk Analytics becomes an administrator user. The administrator user can then invite other users to Risk Analytics and can assign them a user or administrator role.

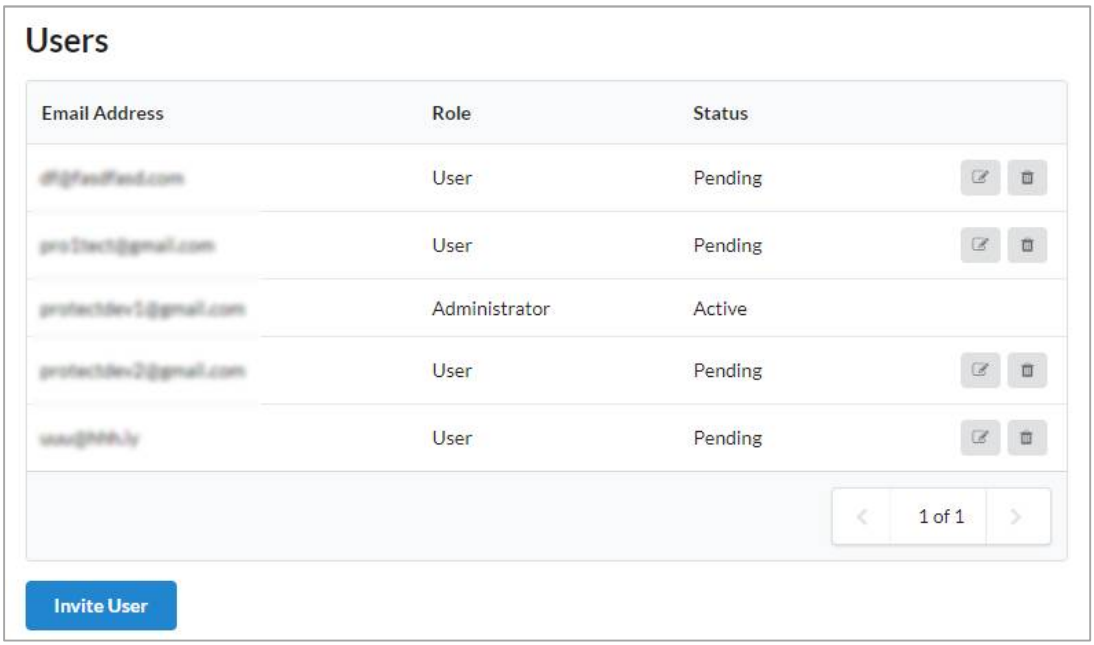
- Users with an **Administrator** role can access all tabs in the Risk Analytics console so they can build and run queries, save queries, monitor the status of the Risk Analytics system and configure settings. They can also invite other users to Risk Analytics.
- Users with a **User** role can access two tabs in the Risk Analytics console so they can build, run and save queries.

To invite people to Risk Analytics:

1. Log into the Risk Analytics console, select **Settings** and then **Users**.
2. Click **Invite User**.

3. Enter the email address of the person you want to invite to Risk Analytics.
4. Select whether you want the invited user to have a **User** or **Administrator** role.

5. Click **OK**. An invitation is sent to the email address inviting the recipient to join Risk Analytics. Until the recipient accepts, you will see them in the user list with the status “Pending”.

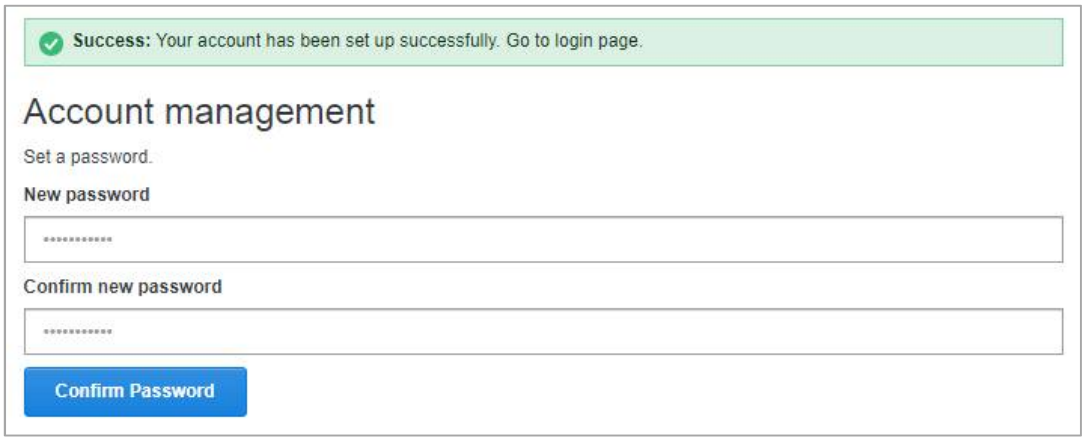


Tip! *You can delete a user or change their role at any time.*

What the invited user sees

The invited user will receive an email with a link to join Risk Analytics. Once they click the link, they are prompted to create a login password.

They must enter a password twice and click **Confirm Password**.

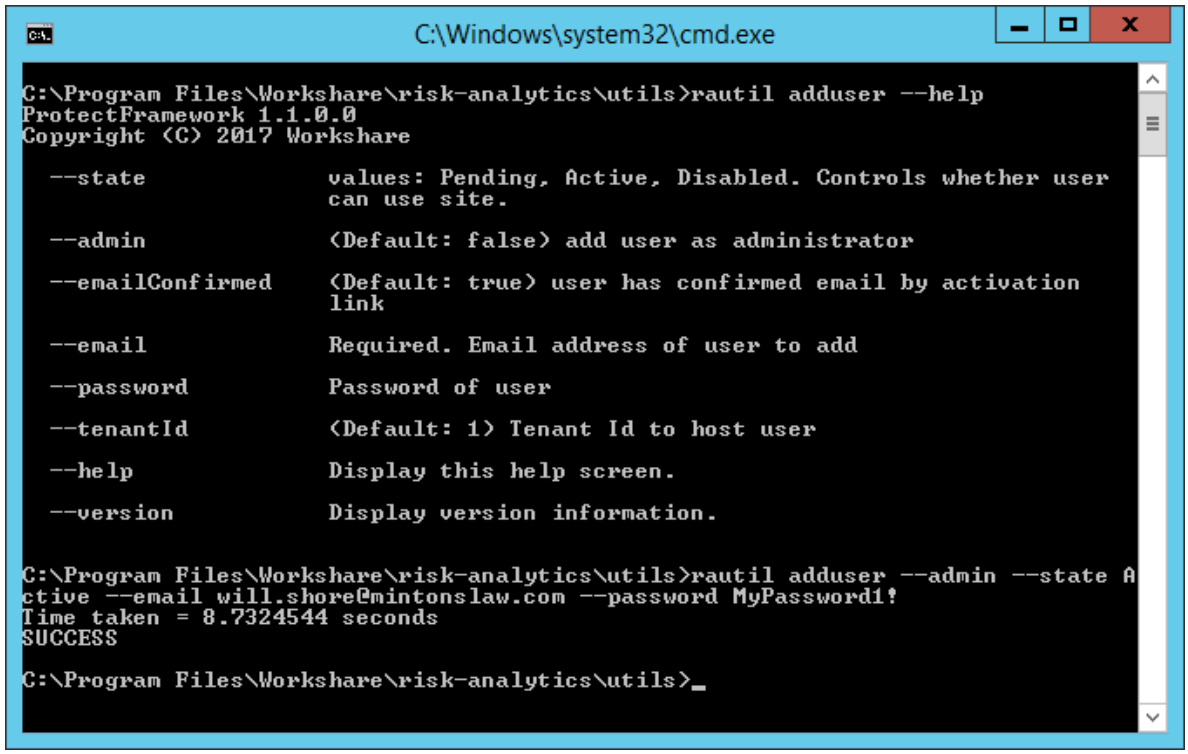


Then the user can click **Go to login page** in the Success message and log in to Risk Analytics using their email address and password.

Command utility to add users

Alternatively, you can use a command line utility to add a user and set a password. Then you must send the user a link to Risk Analytics and details of the password you have set for them.

To add users using the command line, follow the example below:

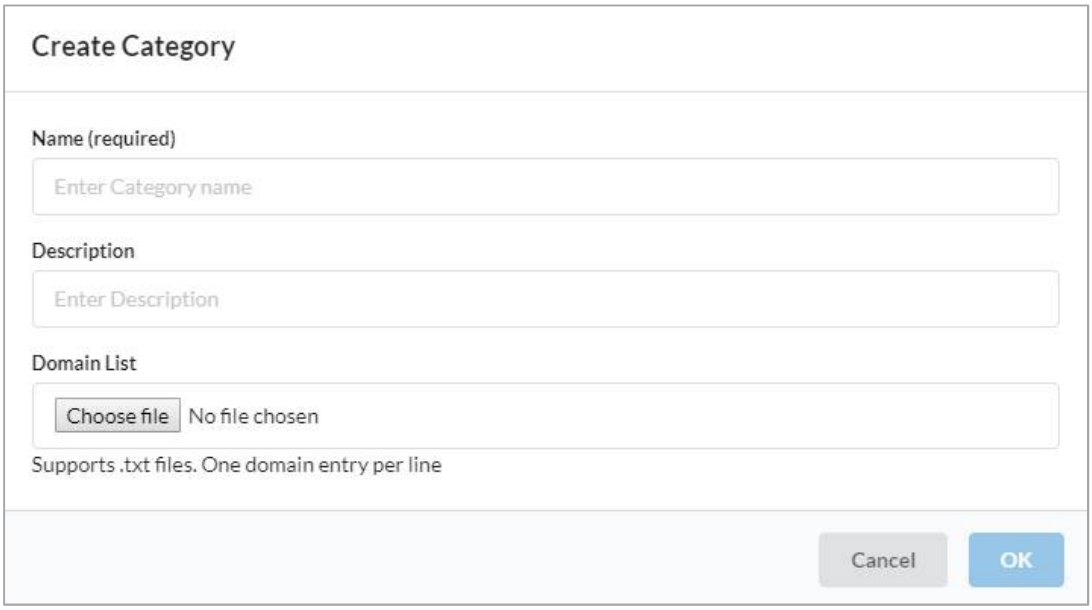


Domain Classification

You identify and classify email domains in order to run queries against a particular email domain. For example, classify a group of domains as “Newspapers/Press” or another as “Competitors”.

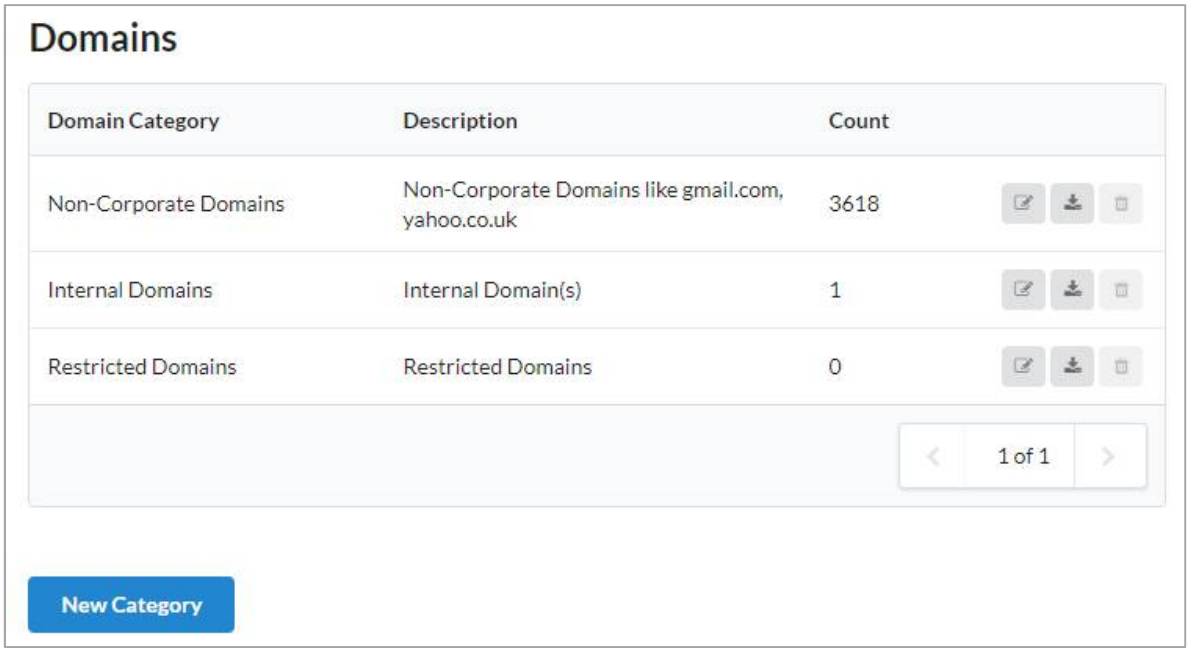
To classify domains:

1. First of all, create a text file listing the domains you want to monitor. You can enter multiple domains but each must be on a separate line. You can also download a list of domains from a blacklisting services site.
2. In the Workshare Risk Analytics console, select **Settings**.
3. Select **Domains**.
4. Click **New Category**.



5. Add a name for your new domain list and a suitable description.
6. Click **Choose File** and browse to your saved text file.

7. Click **OK**.



You can now select this domain category when creating a report.

***Note**: You can edit a domain category or delete it. You can also download the text file.*

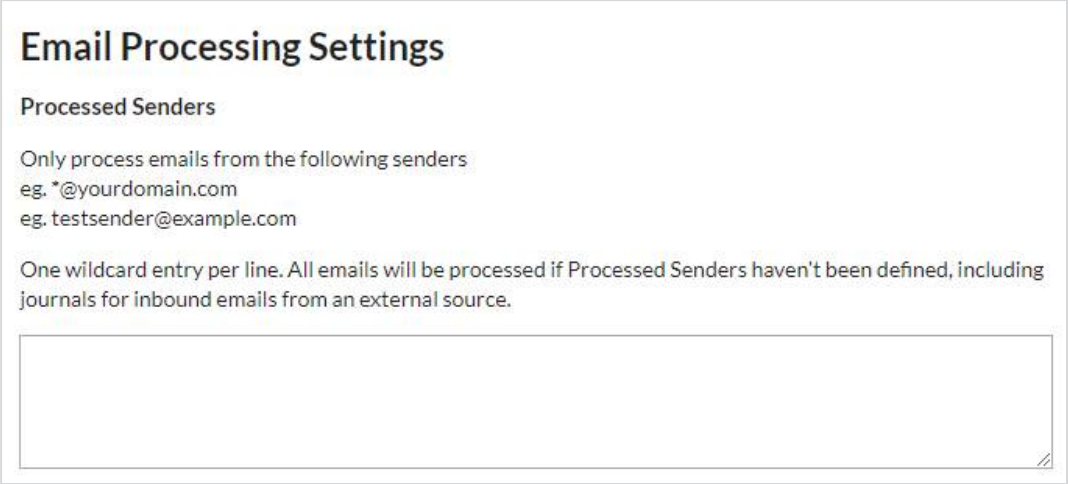
Selecting Emails to Monitor

By default, Risk Analytics processes journals (copies) of all outbound email sent externally. You can configure Risk Analytics to process only the email from selected senders.

To select emails:

1. In the Risk Analytics console, select **Settings**.

2. Select **Email processing**.



3. In the **Processed Senders** area, enter the domains you want to monitor. By default, Risk Analytics processes all emails if nothing is specified here. You can specify a whole domain, such as *@workshare.com or just a couple of users on that domain. When entering multiple domains, put each on a separate line.
4. Click **Save Changes**.

Protect Server configuration

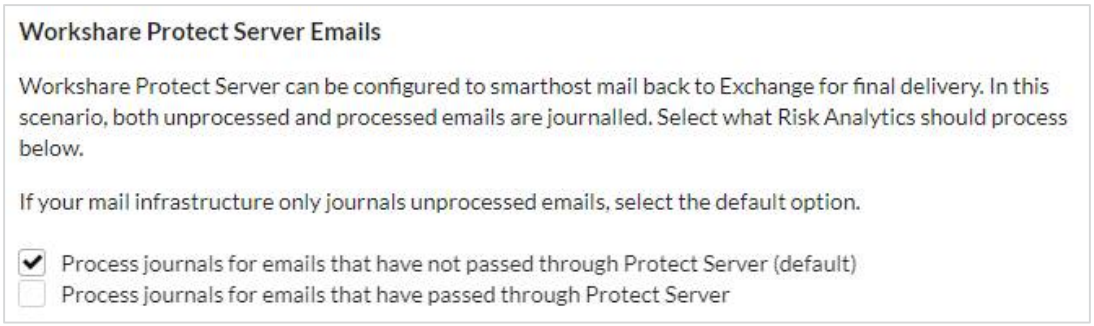
When you have Workshare Protect Server and the Workshare Protect Routing Agent set up in your email environment, a journal is made of emails going into Protect Server and again when they come out, before they are sent on for final delivery. You can select whether you want Risk Analytics to process both these journals or just one. By default, Risk Analytics processes journals of emails made before the email is processed by Protect Server.

***Note**: This is only when you're working with Protect Server AND the Routing Agent.*

To configure processing with Protect Server:

1. In the Risk Analytics console, select **Settings**.

2. Select **Email processing**.



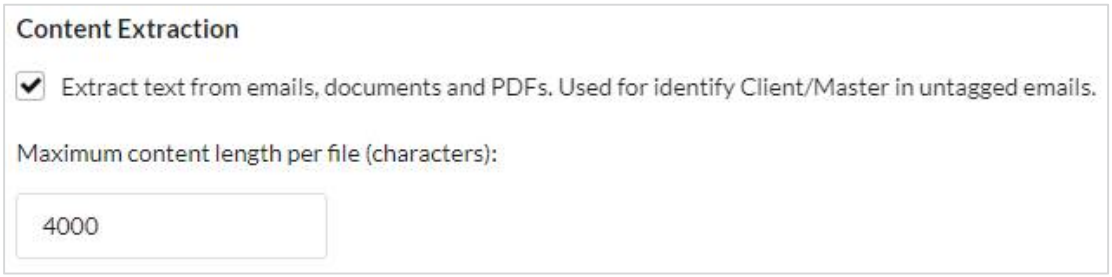
3. In the **Workshare Protect Server Emails** area, select either or both of the checkboxes.
   - **Process journals for emails that have not passed through Protect Server**: Risk Analytics processes journals (copies) of emails made before the email is processed by Protect Server.
   - **Process journals for emails that have passed through Protect Server**: Risk Analytics processes journals (copies) of emails made after the email has been processed by Protect Server.
4. Click **Save Changes**.

Content extraction

You can configure Risk Analytics to pull content from the body of the attachment to get more information about the document. This could help to identify the matter ID or the type of document being sent.

To enable content extraction:

1. In the Risk Analytics console, select **Settings**.
2. Select **Email processing**.



3. In the **Content Extraction** area, select the checkbox.
4. Click **Save Changes**.

Workshare Ltd.
© 2018. 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.

Revisions
Published for Workshare Risk Analytics 1.1: 01/02/18
Revised for Workshare Risk Analytics 1.3: 15/05/18

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