Workshare

Workshare Protect 8

User Guide

Version 4.0 | October 2014

Company Information

Workshare Protect 8 User Guide

Workshare Ltd. (UK)
20 Fashion Street
London
E1 6PX
UK

Workshare Inc. (USA)
625 Market Street, 15th Floor
San Francisco
CA 94105
USA

Workshare Website: www.workshare.com

Trademarks

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.

Disclaimers

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.

Copyright

Table of Contents

Chapter 1. Introducing Workshare Protect

This chapter introduces Workshare Protect, providing an overview of how it works as well as a summary of the key features and benefits. It includes the following sections:

- **What is Workshare Protect?**, below, introduces Workshare Protect.
- **Workshare Protect Functionality**, page 7, describes the different functionality available with Workshare Protect.

What is Workshare Protect?

Workshare Protect is seamlessly integrated with Microsoft Office and automatically enforces company security policy at end-user workstations. Rather than simply block information flow, Workshare Protect warns and educates users in real-time about sensitive information and, if authorized, lets users decide how to treat the content. Workshare Protect provides:

- **Hidden Data/Metadata Removal**
  - Policy driven content risk management
  - Discovery and removal of hidden data and visible content leaks
  - Complete metadata protection for Microsoft Office and PDF documents
- **Storage of Attachments in Workshare Online**
  - Uploading attachments to Workshare Online and sending recipients links to the documents
  - Frees users from having to send attachments by email
  - Facilitating the sharing of files outside of email
- **Tamper-Proof PDF Creation**
  - Converting any document to Workshare's secure PDF from any application
  - Ensuring flexible publishing and complete PDF security options
  - Enforcing automatic conversion of documents to secure PDF before they can be emailed
- **Stopping of Violations in Real Time**
  - Enabling users to fix potential problems with manual redaction options
  - Password-protecting documents or restricting them from being sent externally, or at all.
- **Content Protection and Control**
  - Content analysis and data leak prevention
  - Automatically stopping leaks of intellectual property at their origin
  - Keeping data safe and secure from embarrassing public disclosures
  - Monitoring all communications at the client level
  - Providing alerts for data in use, at rest, and in motion—even when disconnected from the network

***Note**: Workshare Protect can be installed without Microsoft Office integration. In this case, the metadata removal functionality is only available when sending emails and PDF creation is available through the right-click menu.*

Workshare Protect Functionality

Workshare Protect displays a simple and intuitive panel within Microsoft Word, Excel and PowerPoint enabling users to take advantage of available Workshare Protect functionality from within the application.

The Workshare Panel is task-oriented, guiding users through their document tasks in a clear, step-by-step format. Users may select Workshare Protect functions in any order, or simply use a single function.

Discovering Content Risk

Workshare Protect provides comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well visible sensitive data. Content risk is defined in security policies. Hidden sensitive data may include information such as track changes, author's name, server names, keywords, routing slips and authoring trails.

Workshare Protect enables the discovery of content risk in the following ways:

- **Content Risk Reports**: Workshare Protect integrates with Microsoft Office providing an option to display a comprehensive report of all the content risk in a document while it is open in Microsoft Word, Excel and PowerPoint. Content risk is displayed according to its risk level (high, medium, low).
- **Email Protection**: Workshare Protect prevents users from accidentally emailing confidential information by alerting users before the email is sent when an email or its attachment breaches security policies. Depending on the actions defined for policy breaches, emails may be blocked or sensitive data removed. Security policies can specify different actions when a document is sent internally or externally. For example, it may not be acceptable for hidden server names and users details to be included in documents sent externally, but it may be fine to leave those details in documents sent within an organization.

Workshare Protect comes with a pre-defined default security profile (collection of policies).

Interactive Protect

Interactive Protect offers you options to control your documents and secure attachments before sending your email. It simplifies metadata cleaning, avoids email pop-ups, and eliminates MS Outlook add-in issues.

Workshare Protect scans documents as soon as they are added as attachments to an email. Users are made aware of the risk involved and given the option to make informed decisions to decide what metadata to remove. BEFORE clicking Send. Users can then preview processed documents before they are sent.

Using the Interactive Protect panel displayed on the right of the message window, users can clean metadata from attachments, convert attachments to PDF or PDF/A, and compress attachments into one zip file. Additionally, users can securely transfer attachments to a secure location in Workshare Online and send recipients a link to that location.

Interactive Protect is implemented by selecting **Interactive Protect** for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).).

Secure File Transfer

The Secure File Transfer functionality provides the ability to upload attachments to Workshare Online and send recipients a link to the documents in Workshare. This means that valuable email storage isn't taken up with multiple versions of large attachments. Additionally, attachments are stored in a single place which enables efficient and trouble-free collaboration. Workshare can also clean attachments before uploading them to Workshare Online.

Secure File Transfer is initiated from within the familiar environment of Microsoft Outlook. The feature is implemented through the use of two additional profiles – **Secure File Transfer** and **Clean & Secure File Transfer** that are available in the *Protect Profile* dialog. The various configuration options relating to this functionality are found in a new sub-category – **Protection**> **Secure File Transfer** in the Workshare Configuration Manager and the functionality is enabled/disabled using the **Show Secure File Transfer profiles in Protect Profile dialog** parameter (**Protection**>**Administration** category).

Manual Redaction

Workshare Protect provides the functionality to redact/black out selected content in Microsoft Word (DOC and DOCX) documents. Redacting text is to black out the text so that it is no longer discernible.

PDF Conversion

Workshare Protect enables you to quickly and easily convert Microsoft Office documents into PDF or PDF/A files. This Workshare Protect functionality is available from within Microsoft Word, Excel and PowerPoint environments and by right-clicking closed Microsoft Word, Excel and PowerPoint files on your desktop or DMS. Additionally you can combine multiple files into a single PDF – a useful tool at the close of a project or when creating a report that involves documents, spreadsheets and graphics.

Document Classification

Workshare Protect enables you to restrict access to sensitive business documents by classifying documents. This classification can prevent documents from being emailed either to any user, or to external users. Workshare Protect provides the following default classification levels:

- For Internal Use
- Confidential
- Highly Confidential
- External Restriction
- Full Restriction

Chapter 2. Getting Started

This chapter describes the Workshare Protect working environment and provides an overview of the tools available. It includes the following sections:

- **Launching Workshare Protect**, below, describes how to access Workshare Protect functionality.
- **Workshare Panel**, page 10, describes the Workshare Panel and the options available from it.
- **Workshare Tab**, page 12, describes the options available in the Workshare tab.
- **Enabling Workshare Protect Functionality**, page 13, describes how to ensure that Workshare Protect functionality is fully enabled.

Launching Workshare Protect

Workshare Protect can integrate with Microsoft Word, Excel, PowerPoint and Outlook. To this end, there is no independently accessed user interface for Workshare Protect - the user interface is accessed from within Microsoft Word, Excel, PowerPoint or Outlook and is available from all documents.

***Note**: If your Workshare Protect is not integrated with Microsoft Word, Excel, PowerPoint and Outlook, refer to your system administrator.*

The Workshare Protect user interface adopts a task-oriented approach guiding you through each process one step at a time and providing clear explanations at each step. This provides a steady flow to your work with no need to move between interfaces or waste time deducing functionality.

After you have installed Workshare Protect, the Workshare tab is added to the Ribbon in your Microsoft Office applications - Word, Excel and PowerPoint. Click **Toggle Panel** in the Workshare tab and the Workshare Panel is displayed down the left side of the window.

The addition of Workshare Protect does not affect the standard functionality of Microsoft Word, Excel or PowerPoint. You can operate these applications as usual and access the Workshare Protect functionality as required.

Workshare Protect functionality can also be accessed in the following ways:

- Right-click closed Microsoft Word documents and select **Convert to PDF with Workshare** or **Send to/Workshare Batch Clean**.
- Right-click closed Microsoft Excel or PowerPoint documents and select **Convert to PDF with Workshare** or **Send to/Workshare Batch Clean**.
- Right-click closed PDF documents and select **Open in Word with Workshare** or **Send to/Workshare Batch Clean**.

***Note**: Workshare Protect can be installed without Microsoft Office integration. In this case, the Workshare Panel and Workshare tab/menu are not available. The Workshare metadata removal functionality is only available when sending emails.*

Start Menu

After you have installed Workshare Protect, the following elements are added to the Start menu under Workshare:

- Workshare Batch Clean
- Workshare Configuration
- Workshare Configuration Assistant
- Help

Batch Clean

Workshare Batch Clean is a tool that cleans hidden data, such as versions, templates, comments, hidden text, reviewer and author information, from multiple Microsoft Office documents at the same time. Refer to Batch Cleaning, for further information.

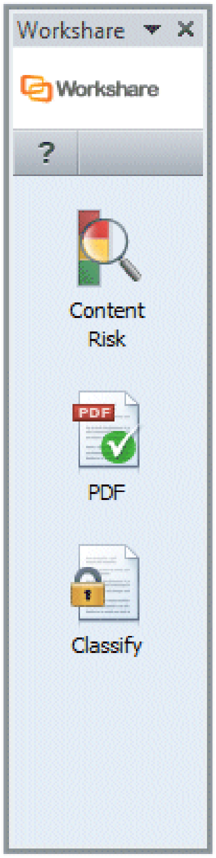
Workshare Panel

The Workshare Panel, displayed by default down the left side of the Microsoft Word, Excel and PowerPoint windows, provides access to Workshare Protect functionality and is your guide, prompting you through each step of any given process.

The content of the Workshare Panel varies according to the application and the functionality selected.

You can display/hide the Workshare Panel by clicking **Toggle Panel** in the Workshare tab, **Options** group.

In Microsoft Office, the Home page of the Workshare Panel, shown below, provides quick access to the functionality of Workshare Protect, as follows:



Content Risk: Enables you to display a report of all the content risk in a document as well as remove selected hidden data from the document. Refer to Displaying Content Risk in Microsoft Word for further information.

PDF: Enables you to convert documents to PDF. Refer to Overview – Converting to PDF for further information.

Classify: Enables you to classify your documents, which can restrict whether or not they can be emailed. Refer to Document Classification for further information.

> ***Tip!*** *The Workshare Panel can float over other windows. Click and drag the title bar of the Panel to move it to a different location.*

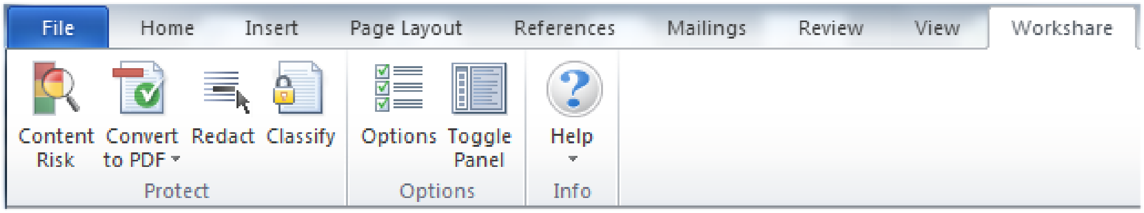
> ***Note:*** *All of these options are configurable. You can configure whether each individual option is available from the* ***General > User Interface*** *category in the Workshare Configuration Manager. Refer to* Workshare Configuration Options *for further information.*

There is a Help button ? displayed at the top of every page in the Workshare Panel that provides access to online help as well as a close button that enables you to close/hide the Workshare Panel. Additionally, at the top of all pages of the Workshare Panel except the Home page, the following links are displayed:

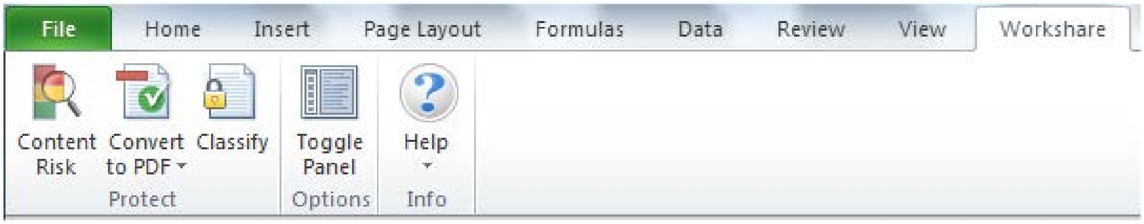
⌂	Return to the Home page of the Workshare Panel.
←	Return to the previously displayed page of the Workshare Panel.

Workshare Tab

Microsoft Word



Microsoft PowerPoint and Excel



Many of these options are configurable from the **General > User Interface** category in the Workshare Configuration Manager. Refer to *Workshare Configuration Options* for further information.

The *Workshare* tab includes the following options:

Group	Item	Description
Protect	**Content Risk**	Enables you to display a report of all the content risk in a document as well as remove selected hidden data from the document. Refer to Displaying Content Risk in Microsoft Word for further information.
	Convert to PDF	Enables you to convert documents to PDF as well as convert a document to PDF and then add the PDF as an attachment to an email. Refer to Creating PDFs for further information.
	Redact	Enables you to redact/black out select text. Refer to Manual Redaction for further information.
	Classify	Enables you to classify your documents, which can restrict whether or not they can be emailed. Refer to Document Classification for further information.
Options	**Options**	Enables you to configure system parameters in the Workshare Configuration Manager. Refer to Introducing the Workshare Configuration Manager for further information.
	Toggle Panel	Displays/hides the Workshare Panel down the left side of the Microsoft Word window. The Workshare Panel is displayed with its Home page open. Refer to Workshare Panel.
Info	**Help**	Provides access to version, copyright and license information about Workshare Protect.

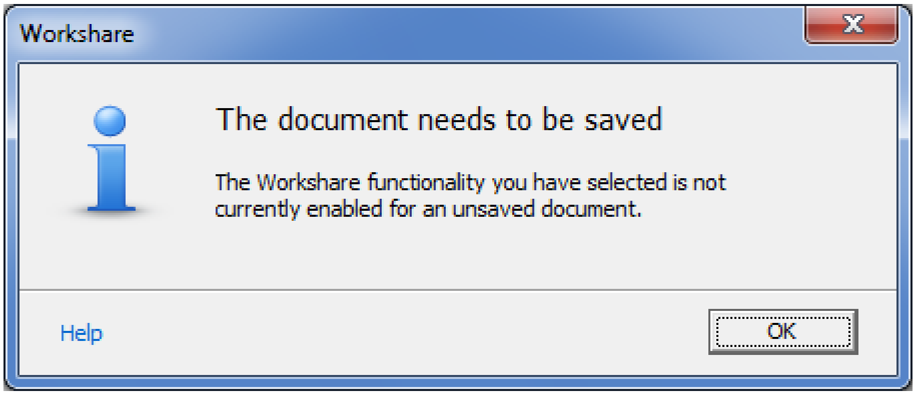
Enabling Workshare Protect Functionality

To ensure Workshare Protect functionality is *fully* enabled, you should work with saved documents and on the latest version of a document.

Saved Documents

You must be working on a *saved* Microsoft Word document in order for the Workshare Protect functionality to be fully enabled.

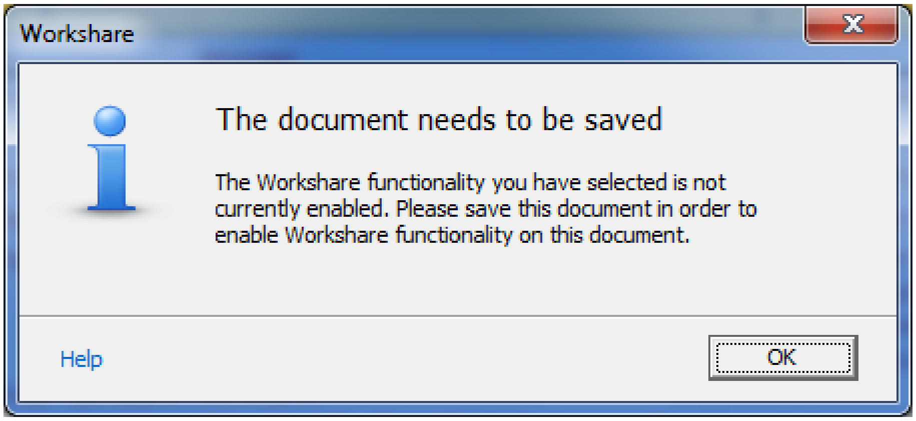
If you are working in Microsoft Office on an unsaved document, Workshare Protect functionality is not fully enabled. If you select **Classify**, the following message is displayed:



The document needs to be saved

The Workshare functionality you have selected is not currently enabled for an unsaved document.

If you open a document directly from an email, it is only a temporary document that is saved in a temporary location. In this scenario, if you select **Classify**, the following message is displayed:



The document needs to be saved

The Workshare functionality you have selected is not currently enabled. Please save this document in order to enable Workshare functionality on this document.

Chapter 3. Managing Content Risk in Documents

This chapter describes how to view the content risk in documents as well as remove selected content risk from a document. It includes the following sections:

- **Overview**, below, introduces the ways in which Workshare Protect enables you to protect documents by viewing and removing sensitive content risk.
- **Displaying Content Risk in Microsoft Word**, page 14, describes how to discover all content risk in a Microsoft Word document.
- **Displaying Content Risk in Microsoft Excel and PowerPoint**, page 16, describes how to discover all content risk in a Microsoft Excel or PowerPoint document.
- **Cleaning Hidden Data**, page 17, describes how to remove selected types of hidden data from a document and from multiple documents.
- **Manual Redaction**, page 27, describes how to manually redact selected words or other content.

Overview – Managing Content Risk in Documents

Workshare Protect provides comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well visible sensitive data. Hidden sensitive data may include information such as track changes, author's name, server names, keywords, routing slips and authoring trails.

Workshare Protect enables the discovery of content risk in the following ways:

- **Content Risk Reports**: Workshare Protect integrates with Microsoft Office providing an option to display a comprehensive report of all the content risk in a document while it is open in Microsoft Word, Excel and PowerPoint. Content risk is displayed according to its risk level (high, medium, low).
- **Email Protection**: Workshare Protect prevents users from accidentally emailing confidential information by alerting users before the email is sent when an email or its attachment breaches security policies. Refer to Overview – Protecting Email Attachments.

In addition, Workshare Protect provides manual redaction functionality which enables you to redact selected words or sentences or other content as required.

Displaying Content Risk in Microsoft Word

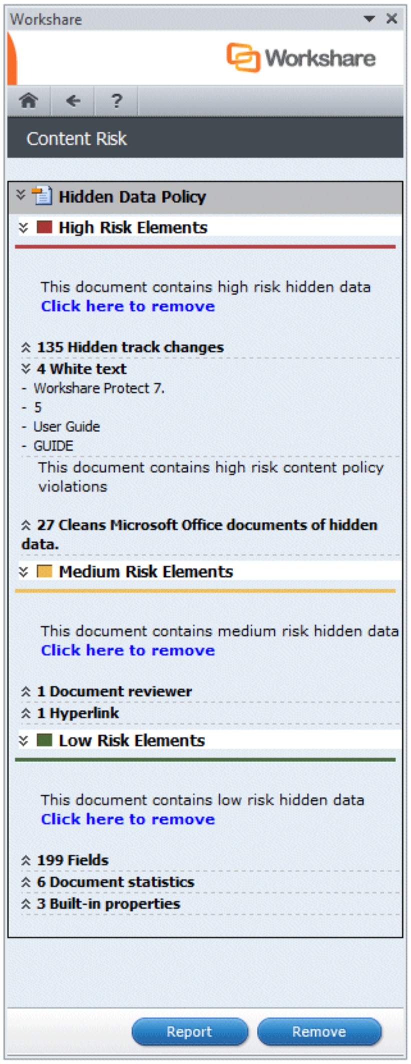
Workshare Protect integrates with Microsoft Word to provide an option to discover and view content risk in a document. You can also display a comprehensive report of all the content risk in a document.

To discover content risk in your Microsoft Word document:

1. Open your document in Microsoft Word and click **Content Risk**, (**Protect** group) in the *Workshare* tab or click **Content Risk** in the Home page of the Workshare Panel.

***Note**: You can also click **Content Risk** from other pages in the Workshare Panel.*

Workshare Protect checks the document for content risk. This process may take a few moments if your document is large or if it contains large amounts of content risk. Once the discovery process is complete, the Content Risk page of the Workshare Panel is displayed showing a summary of the content risk found.



︾ Hidden Data Policy

︾ 🟥 High Risk Elements

This document contains high risk hidden data
Click here to remove

︽ 135 Hidden track changes
︾ 4 White text
- Workshare Protect 7.
- 5
- User Guide
- GUIDE

This document contains high risk content policy violations

︽ 27 Cleans Microsoft Office documents of hidden data.

︾ 🟨 Medium Risk Elements

This document contains medium risk hidden data
Click here to remove

︽ 1 Document reviewer
︽ 1 Hyperlink

︾ 🟩 Low Risk Elements

This document contains low risk hidden data
Click here to remove

︽ 199 Fields
︽ 6 Document statistics
︽ 3 Built-in properties

The content risk found is divided into high risk, medium risk and low risk.

2. To display details of the content risk found, click ︽ to the left of the content risk type.
3. To remove hidden data from the document, use the **Remove** button. Refer to Cleaning Hidden Data, for more details.

***Note:** You can click **Report** to create a risk report that provides a full account of the different types of content risk in a document.*

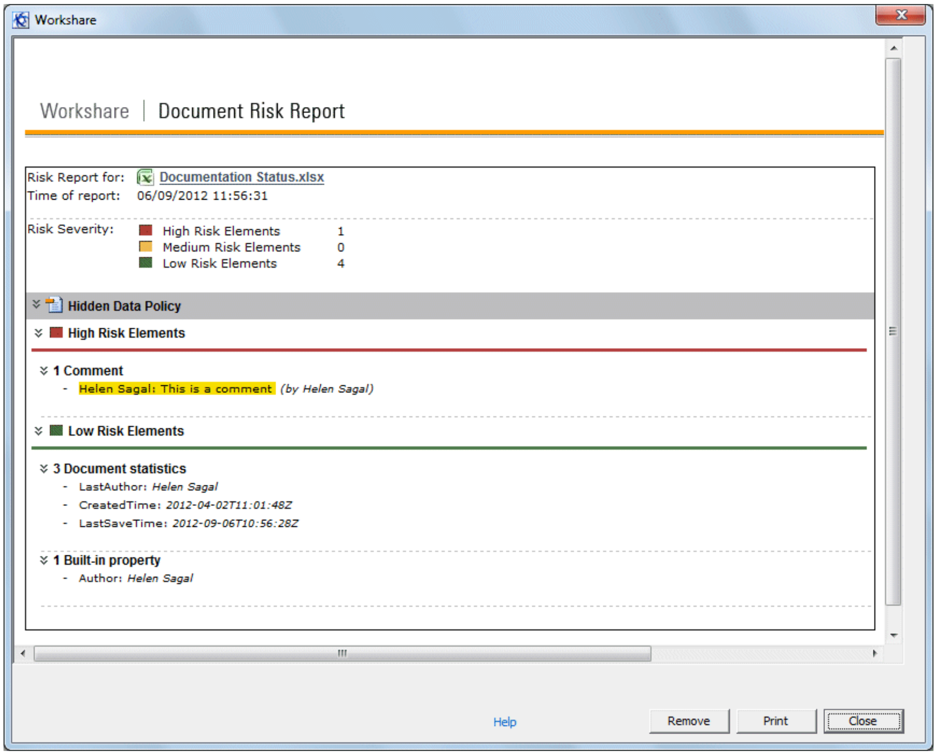
Displaying Content Risk in Microsoft Excel and PowerPoint

Workshare Protect integrates with Microsoft Excel and PowerPoint to provide an option to discover and view content risk in a document. The content risk is displayed in a comprehensive report.

To discover content risk in your Microsoft Excel or PowerPoint document:

1. Open your document in Microsoft Excel or PowerPoint and click **Content Risk**, (**Protect** group) in the *Workshare* tab, or click **Content Risk** in the Home page of the Workshare Panel.

   Workshare Protect checks the document for content risk. This process may take a few moments if your document is large or if it contains large amounts of content risk. Once the discovery process is complete, the Document Risk Report is displayed showing the details of the content risk found:



Workshare | Document Risk Report

Risk Report for: Documentation Status.xlsx
Time of report: 06/09/2012 11:56:31

Risk Severity:

🟥	High Risk Elements	1
🟨	Medium Risk Elements	0
🟩	Low Risk Elements	4

Hidden Data Policy

High Risk Elements

1 Comment
- Helen Sagal: This is a comment *(by Helen Sagal)*

Low Risk Elements

3 Document statistics
- LastAuthor: *Helen Sagal*
- CreatedTime: *2012-04-02T11:01:48Z*
- LastSaveTime: *2012-09-06T10:56:28Z*

1 Built-in property
- Author: *Helen Sagal*

   The content risk found is divided into high risk, medium risk and low risk.

2. To print the report, click **Print**.

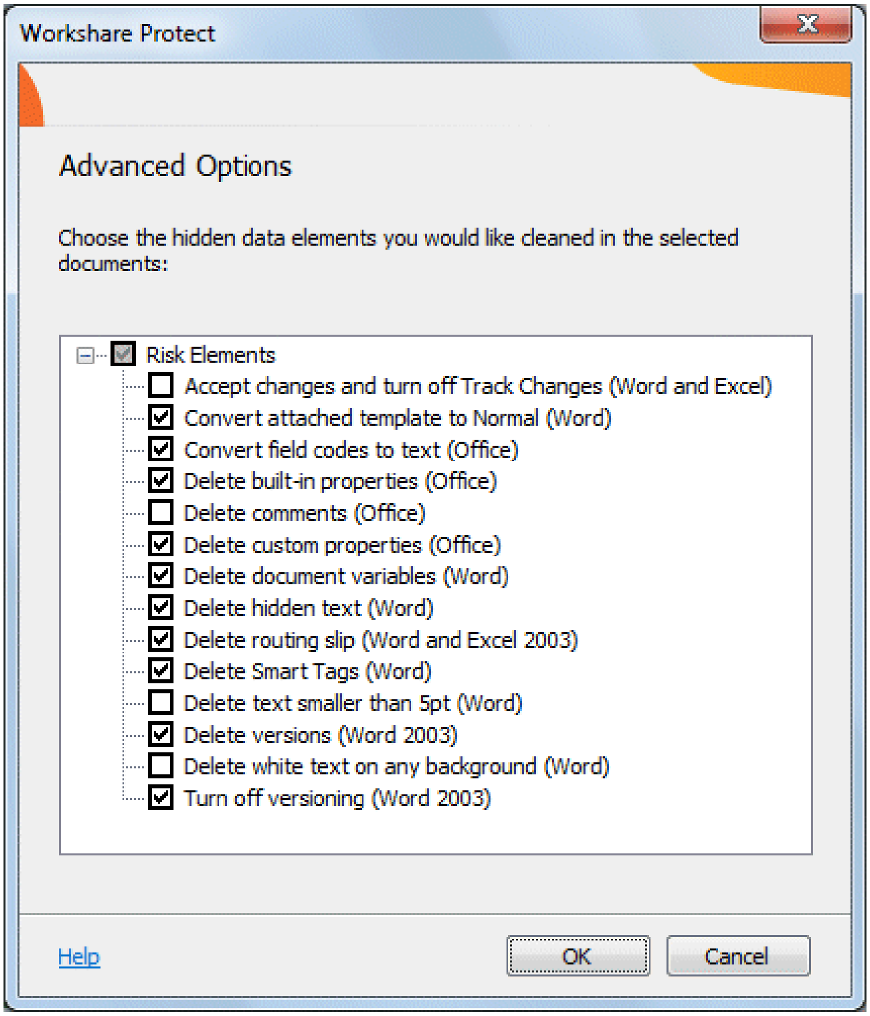
3. To remove the hidden data from the Microsoft Excel or PowerPoint document, click **Remove**. Refer to Cleaning Hidden Data for further information.

Cleaning Hidden Data

In Microsoft Office documents, once you have discovered the content risk in a document, you can remove selected types of hidden data as required. If you want to remove hidden data from PDF files or from multiple Microsoft Office documents, you can use the Workshare Batch Clean tool. Refer to Batch Cleaning.

To remove hidden data:

1. In Microsoft Word, click **Remove** in the Content Risk page. In Microsoft Excel or PowerPoint, click **Remove** in the Document Risk Report. The *Advanced Options* dialog is displayed.



Advanced Options

Choose the hidden data elements you would like cleaned in the selected documents:

- ☑ Risk Elements
  - □ Accept changes and turn off Track Changes (Word and Excel)
  - ☑ Convert attached template to Normal (Word)
  - ☑ Convert field codes to text (Office)
  - ☑ Delete built-in properties (Office)
  - □ Delete comments (Office)
  - ☑ Delete custom properties (Office)
  - ☑ Delete document variables (Word)
  - ☑ Delete hidden text (Word)
  - ☑ Delete routing slip (Word and Excel 2003)
  - ☑ Delete Smart Tags (Word)
  - □ Delete text smaller than 5pt (Word)
  - ☑ Delete versions (Word 2003)
  - □ Delete white text on any background (Word)
  - ☑ Turn off versioning (Word 2003)

   A complete list of hidden data that can be removed, reset or converted is listed in the dialog. For a full description of the different options, refer to Cleaning Options.

2. Select the hidden data you want to remove by selecting the checkboxes to the left of the hidden data options.

3. After making your selection, click **OK**. The selected hidden data is removed from the document.

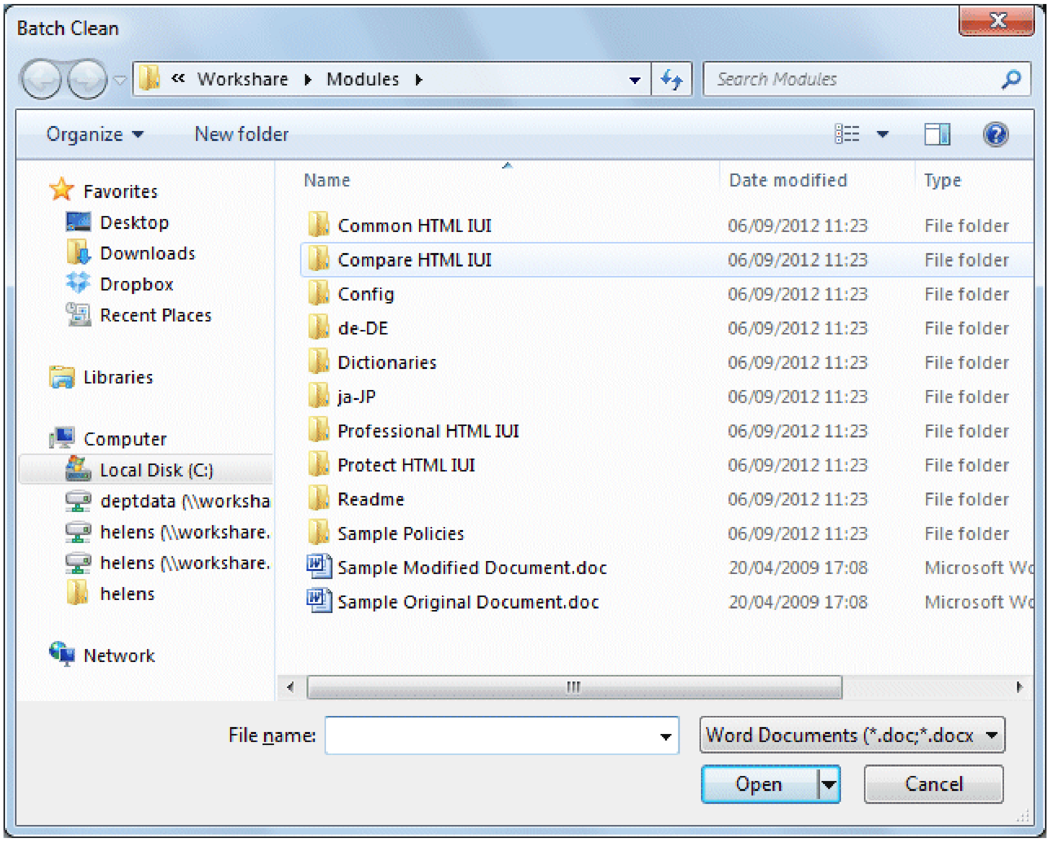
Workshare Protect may take a few moments to clean you document depending on the size of the document and the amount of hidden data to be removed. The Content Risk page/Document Risk Report is updated after the document has been cleaned to show any remaining content risk. After cleaning, the document with hidden data removed is still stored in memory only. If you want to keep the cleaned document, you now have to save the document.

Batch Cleaning

If you want to remove the same types of hidden data from several documents, you can use the Workshare Batch Clean tool to clean multiple documents (up to 256) simultaneously.

To clean multiple documents:

1. From the Start menu, select **Programs**, **Workshare**, and then **Workshare Batch Clean**. The *Batch Clean* dialog is displayed.



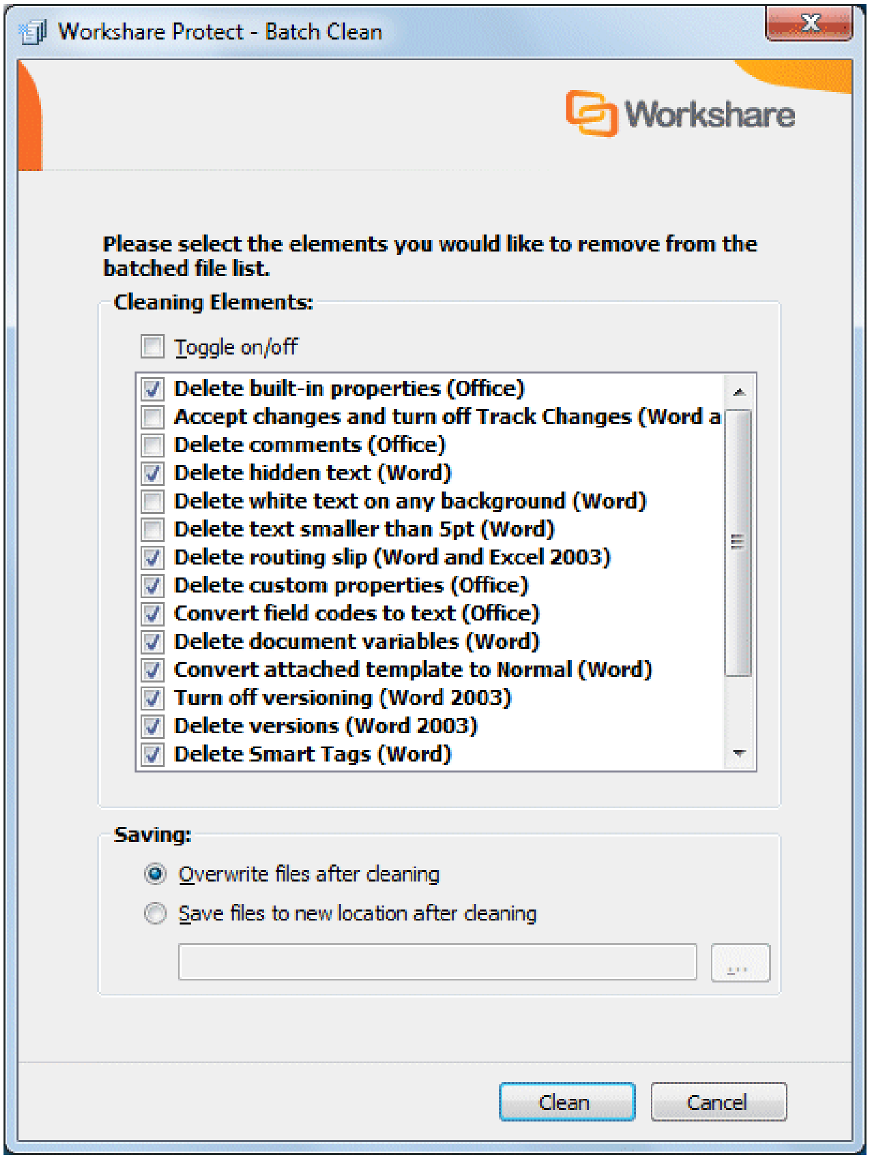
Name	Date modified	Type
Common HTML IUI	06/09/2012 11:23	File folder
Compare HTML IUI	06/09/2012 11:23	File folder
Config	06/09/2012 11:23	File folder
de-DE	06/09/2012 11:23	File folder
Dictionaries	06/09/2012 11:23	File folder
ja-JP	06/09/2012 11:23	File folder
Professional HTML IUI	06/09/2012 11:23	File folder
Protect HTML IUI	06/09/2012 11:23	File folder
Readme	06/09/2012 11:23	File folder
Sample Policies	06/09/2012 11:23	File folder
Sample Modified Document.doc	20/04/2009 17:08	Microsoft Wo
Sample Original Document.doc	20/04/2009 17:08	Microsoft Wo

Note: *To view more document types, select* ***All Office files*** *from the* ***Files of type*** *dropdown list. If unsupported file types are selected for batch cleaning, they will be ignored.*

2. Select the documents you want to clean. Press **Ctrl** or the Shift key to select multiple documents.

3. Click **Open**. The *Batch Clean* dialog is displayed.

***Tip!** An alternative to steps 1, 2 and 3 is to select the documents in Windows Explorer, then right-click and select **Send To** then **Batch Clean**.*



Please select the elements you would like to remove from the batched file list.

Cleaning Elements:

□ Toggle on/off

☑ Delete built-in properties (Office)
□ Accept changes and turn off Track Changes (Word a
□ Delete comments (Office)
☑ Delete hidden text (Word)
□ Delete white text on any background (Word)
□ Delete text smaller than 5pt (Word)
☑ Delete routing slip (Word and Excel 2003)
☑ Delete custom properties (Office)
☑ Convert field codes to text (Office)
☑ Delete document variables (Word)
☑ Convert attached template to Normal (Word)
☑ Turn off versioning (Word 2003)
☑ Delete versions (Word 2003)
☑ Delete Smart Tags (Word)

Saving:

● Overwrite files after cleaning
○ Save files to new location after cleaning

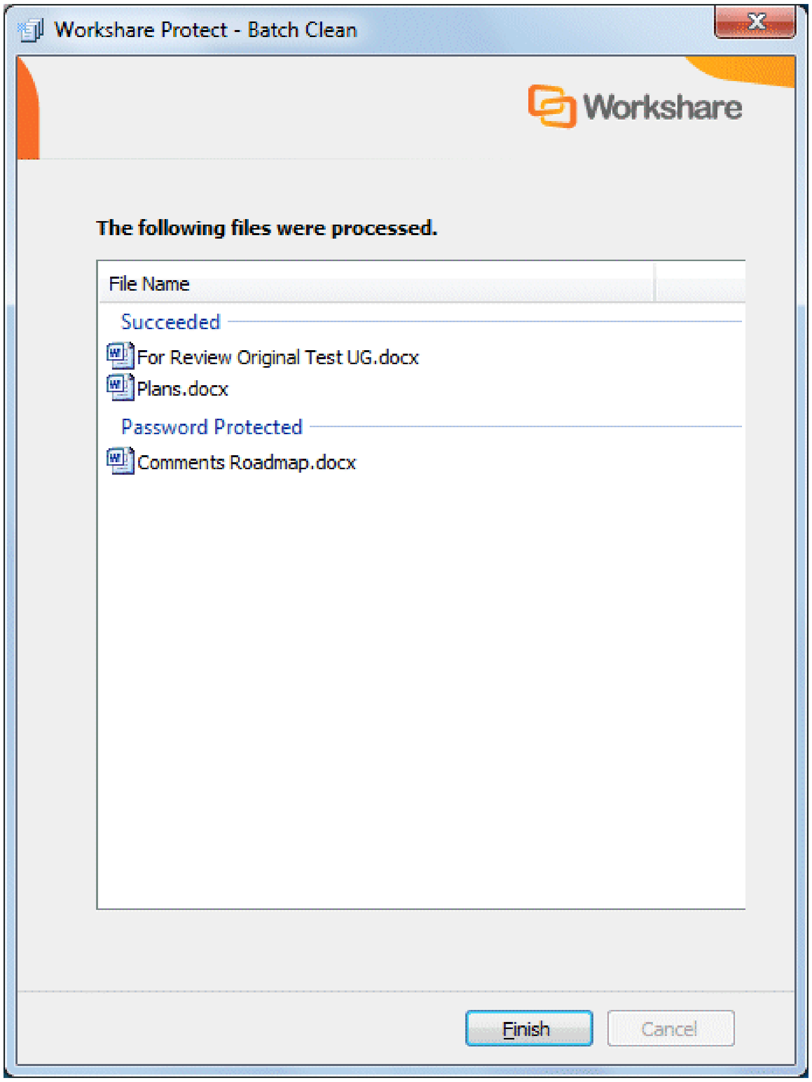
A complete list of hidden data that can be removed, reset or converted is listed in the dialog. For a full description of the different options, refer to Cleaning Options.

4. Select the hidden data you want to remove by selecting the checkboxes to the left of the hidden data options. All the selected files will be cleaned using the same options.

***Tip!** Select the **Toggle on/off** checkbox to select/deselect all the hidden data options.*

5. Select one of the following save options:
   - **Overwrite files after cleaning**: Selecting this option will save the cleaned files over the original files, overwriting the existing version.
   - **Save files to new location after cleaning**: Selecting this option will save the cleaned files to a different location, leaving the original files in their original location and in an uncleaned state. Click the browse button and select the new save location.

6. Click **Clean**. The selected files are cleaned according to your selection. Once the process is complete, a report is displayed indicating which files were cleaned successfully.



The following files were processed.

File Name

Succeeded

For Review Original Test UG.docx

Plans.docx

Password Protected

Comments Roadmap.docx

7. Click **Finish**.

Batch Cleaning Using a Command Line

Batch cleaning can be performed using the command line.

To batch clean using the command line:

1. From the Start menu, select **Run**.
2. Enter **cmd** in the **Open** field and click **OK.**
3. Enter the clean command required. Samples are given below:

- To clean hidden data from the entire hard disk:

  ```
  bc-console.exe “c:\” /s /all
  ```

- To clean all hidden data from a single document:

  ```
  bc-console.exe “<filepath>” /all
  ```

  where <filepath> is the full path to the document to clean.

- To exclude specific data from the cleaning (here comments and track changes are excluded):

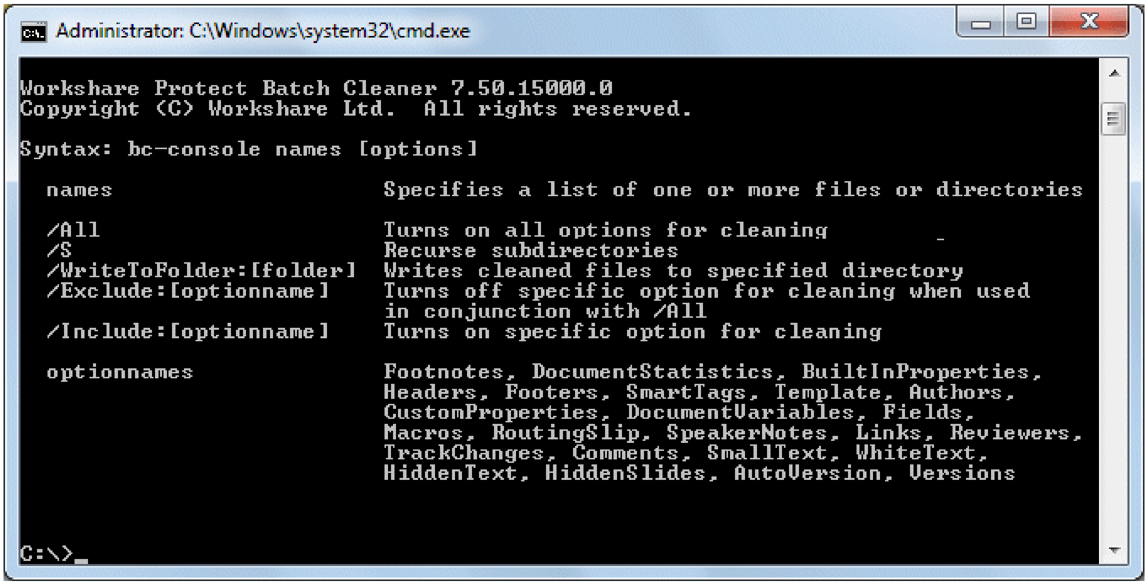
  ```
  Bc-console.exe “<filepath>” /all /exclude:comments /exclude:trackchanges
  ```

- To clean only specified data from the document (here comments and track changes are the data to clean):

  ```
  Bc-console.exe “<filepath>” /include:comments /include:trackchanges
  ```

For a complete list of options, type the following command:

```
Bc-console.exe/
```



```
Workshare Protect Batch Cleaner 7.50.15000.0
Copyright (C) Workshare Ltd.  All rights reserved.

Syntax: bc-console names [options]

  names                      Specifies a list of one or more files or directories

  /All                       Turns on all options for cleaning
  /S                         Recurse subdirectories
  /WriteToFolder:[folder]    Writes cleaned files to specified directory
  /Exclude:[optionname]      Turns off specific option for cleaning when used
                             in conjunction with /All
  /Include:[optionname]      Turns on specific option for cleaning

  optionnames                Footnotes, DocumentStatistics, BuiltInProperties,
                             Headers, Footers, SmartTags, Template, Authors,
                             CustomProperties, DocumentVariables, Fields,
                             Macros, RoutingSlip, SpeakerNotes, Links, Reviewers,
                             TrackChanges, Comments, SmallText, WhiteText,
                             HiddenText, HiddenSlides, AutoVersion, Versions


C:\>_
```

The options are described in the following table:

Option	Description
`/All`	All hidden data is removed from the specified documents. To leave specified types of hidden data in a document, the `/All` command can be used in conjunction with the `/Exclude` command. The `/All` command cannot be used in conjunction with the `/Include` command.
`/S`	Hidden data is removed from sub-folders of the specified folder.
`/WriteToFolder:[folder]`	The cleaned file is saved to a specified location. If this command is not included the original file is overwritten with the cleaned file. Cleaned files saved using the `/WriteToFolder` command will have a flat file structure. If files have the same names, they will be appended with a number.
`/Exclude:[optionname]`	Excludes specified types of hidden data from being removed. The `/Exclude` command is used in conjunction with the `/All` command. The valid types of hidden data that can be excluded are detailed in the **optionnames** list.
`/Include:[optionname]`	Specifies which types of hidden data are to be removed. The `/Include` command is used instead of the `/All` command. The `/Include` command cannot be used with the `/All` command or the `/Exclude` command. The valid types of hidden data that can be specified are detailed in the **optionnames** list.
`optionnames`	The valid types of hidden data that can be used with the `/Exclude` and `/Include` commands. Footnotes, DocumentStatistics, BuiltInProperties, Headers, Footers, SmartTags, Template, Authors, CustomProperties, DocumentVariables, Fields, Macros, RoutingSlip, SpeakerNotes, Links, Reviewers, TrackChanges, Comments, SmallText, WhiteText, HiddenText, HiddenSlides, AutoVersion, Versions

Cleaning Options

The different hidden data cleaning options that are selected when cleaning an individual document or when batch cleaning several documents are explained below:

Option	Description
Accept changes and turn off Track Changes (Word and Excel)	Microsoft Word and Excel. Accepts all revisions made to the document. The revisions are therefore no longer displayed as revisions but rather as text in the document. Track changes is also turned off so that further revisions are not tracked.
Convert attached template to Normal (Word)	Microsoft Word only. Converts the attached template to normal.dot. Automatic style updating is disabled before the template is removed. Therefore the formatting and styles in your document will not be affected by removing the attached template. To view the attached template: Click the File menu/Office Button, select **Options/Word Options** and then select **Add-Ins**. From the **Manage** dropdown list, select **Word Add-ins** and click **Go**.
Convert field codes to text (Office)	Microsoft Word, Excel and PowerPoint. Converts any field codes that exist in a Microsoft Word document to text, for example, hyperlinks, table of contents, index. In Microsoft Excel and PowerPoint, hyperlinks are converted to text. ***Note:*** *For Microsoft Excel and PowerPoint, hyperlinks are the only field codes that exist.* This prevents the field codes from being updated after you have distributed the document. It also prevents errors for fields that reference built-in or custom properties that have been removed. ***Note:*** *You may want to remove some field codes but not others. For example, you may want to clean 'Include text' field codes, but retain the Table of Contents and Page Numbers. To do this you can specify the field codes you want to keep in the* ***Protection > Exclude Metadata*** *category of the Workshare Configuration Manager, and then clean field codes as normal. See Workshare Configuration Options for more details.* To view field codes: Click the File menu/Office Button, select **Options/Word Options** and then select **Advanced**. Select the **Show field codes instead of their values** checkbox in the **Show document content** area.
Delete attachments (PDF)	PDF only. Removes files that are attached to the PDF as a whole. Attachments that are linked to a specific point in a PDF file are not removed. They are treated as markups and will only be removed if the **Delete markups** parameter is selected.
Delete bookmarks (PDF)	PDF. If selected, removes any bookmarks in a PDF file.

Option	Description
Delete built-in properties (Office)	Microsoft Word, Excel and PowerPoint. Removes all summary properties - author, category, comments, company, keywords, manager, title, subject, and hyperlink base; and custom properties – text, date and number. To view built-in properties: In MS Office 2010/2013, click the File menu, select **Info** and then select **Advanced Properties** from the **Properties** dropdown list in the right panel. In the *Properties* dialog, select the **Summary** and **Contents** tabs. In MS Office 2007, click the Office Button, select **Prepare** and then select **Properties**. In the Document Information Panel, select **Advanced Properties** from the **Document Properties** dropdown list. In the *Properties* dialog, select the **Summary** and **Contents** tabs.
Delete comments (Office)	Microsoft Word, Excel and PowerPoint. Removes any comments embedded in the document. To display comments: In MS Office 2010/2013, click the **Review** tab and from the **Show Markup** dropdown list (**Tracking** group), select **Balloons** then **Show Only Comments and Formatting in Balloons**. In MS Office 2007, click the **Review** tab and from the **Balloons** dropdown list (**Tracking** group), select **Show Only Comments and Formatting in Balloons**.
Delete custom properties (Office)	Microsoft Word, Excel and PowerPoint. Removes any custom properties that have been added to the document. To view document properties: In MS Office 2010/2013, click the File menu, select **Info** and then select **Advanced Properties** from the **Properties** dropdown list in the right panel. In the *Properties* dialog, select the **Custom** tab. In MS Office 2007, click the Office Button, select **Prepare** and then select **Properties**. In the Document Information Panel, select **Advanced Properties** from the **Document Properties** dropdown list. In the *Properties* dialog, select the **Custom** tab.
Delete document variables (Word)	Microsoft Word only. Deletes all document variables. Document variables are values stored in Microsoft Word documents that are used by either field codes or macros. These variables may contain confidential information like company names or file locations. Even if field codes and macros are removed, the variables used may remain in the document. Variables can be viewed in Microsoft Word in the Visual Basic Editor.
Delete hidden text (Word)	Microsoft Word only. Removes all text that has been formatted as hidden. To view hidden text: Click the File menu/Office Button, select **Options/Word Options** and then select **Display**. Select the **Hidden Text** checkbox.
Delete markups (PDF)	PDF. If selected, removes any markup in a PDF file. Markup is a tool used to make comments and annotations to PDF documents.

Option	Description
Delete properties (PDF)	PDF. If selected, removes properties in a PDF file. Standard properties are details about a file that help identify it, including its title, subject, author, manager, company, category, keywords, comments, and hyperlink base. ***Note**: Removing properties from a PDF/A file will disable its PDF/A status.*
Delete routing slip (Word and Excel 2003)	Microsoft Word and Excel. Removes all entries from a routing slip, as well as the message subject and text. This can prevent email addresses of colleagues from being unknowingly distributed. This also deletes any envelope information, such as recipients, subject, and introduction, which are used when sending to a mail recipient. Routing slips are not supported in MS Office 2007. To view routing slip entries: From the *File* menu, select **Send To** and then **Routing Recipient**. To view envelope information: From the *File* menu, select **Send To** and then **Mail Recipient**.
Delete Smart Tags (Word)	Microsoft Word only. Removes smart tags from Microsoft Word documents. Smart tags are added to your documents as you create them if the option is enabled. These tags are linked to particular text in a document, such as a name, and allow you to perform certain actions by selecting the link associated with the text. Depending on the smart tag functions you use, they may embed extra hidden information in your document. Smart tags only exist in Microsoft Office XP to 2010. To manage smart tags: In MS Word 2010, right-click a word, select **Additional Actions** and then **Options**. In MS Word 2007, click the Office Button, select **Word Options** and then select **Proofing**. Click the **AutoCorrect Options** button and select the **Smart Tags** tab.
Delete text smaller than 5pt (Word)	Microsoft Word only. Removes all text that has been formatted with a font size less that 5pt (i.e. 4pt and less). Small text can also be detected in Microsoft Excel but it is not cleaned. To view small text: Click the **View** tab, select **Zoom** and specify a percentage greater than 100%.
Delete white text on any background (Word)	Microsoft Word only. Removes all text with a white font that has been formatted with a white background color. To view such text: Click the **Page Layout** tab and select a color from the **Page Color** dropdown list (**Page Background** group).

Option	Description
Delete versions (Word 2003)	Microsoft Word only. Removes any previous versions of the document that you may have saved. Previous versions can be useful while you are developing a document, but often they can contain confidential information that you have removed from the main document. Document versions are not supported in MS Office 2007. To view versions: From the *File* menu, select **Versions**.
Turn off versioning (Word 2003)	Microsoft Word only. Turns off the flag to automatically save a new version of the document every time the document is closed. This applies to local file systems only. Versions can still be saved manually by saving a file with a different name. Versioning is not supported in MS Office 2007.
Delete footers (Excel and PowerPoint)	Microsoft Excel and PowerPoint. Removes any footers included in the sheet or slide. To view headers and footers: Click the **Insert** tab and select **Header & Footer** (**Text** group).
Delete headers (Excel and PowerPoint)	Microsoft Excel and PowerPoint. Removes any headers included in the sheet or slide. To view headers and footers: Click the **Insert** tab and select **Header & Footer** (**Text** group).
Delete links (Excel)	Microsoft Excel only. Converts external links in Microsoft Excel files to text. The following are examples of external links: Link to a cell in another Microsoft Excel document. Named link to a named reference in another Microsoft Excel document. Link to another document. OLE link that inserts another document as an icon. OLE link that inserts another document as text.
Delete hidden slides (PowerPoint)	Microsoft PowerPoint only. Removes hidden slides from Microsoft PowerPoint files. Hidden slides are not required for a slide show (they are not automatically displayed during a slide show) but they may contain confidential information.
Delete Speaker Notes (PowerPoint)	Microsoft PowerPoint only. Deletes all text that appears on the Notes Page in a Microsoft PowerPoint presentation. This is usually used by speakers to remind them of points during a presentation. You may want to remove speaker notes before distributing a presentation, as they are not usually intended for others to read.

Manual Redaction

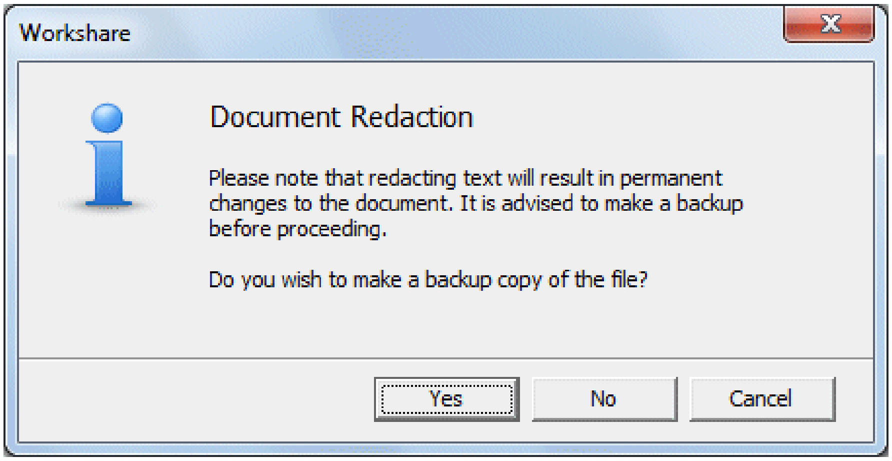
Redacting text is to black out the text so that it is no longer discernible. Workshare Protect provides the functionality to redact/black out selected content in Microsoft Word (DOC and DOCX) documents.

The functionality is available from a right-click menu and also from the Workshare tab.

Redacting text actually replaces the text with "pipes" (||||||) on a black background. Once you make redactions in your document and save it, the redacted text cannot be restored (apart from the immediate possibilities of the Undo action).

To redact selected text:

1. Select the word, sentence or other data that you want to black out.
2. Right-click the selection and select **Redact Text** or click **Redact** in the Workshare tab (**Protect** group). The following message is displayed:



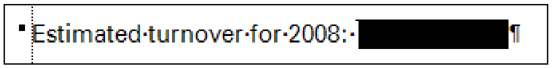
Workshare

Document Redaction

Please note that redacting text will result in permanent changes to the document. It is advised to make a backup before proceeding.

Do you wish to make a backup copy of the file?

3. Click **Yes** to save a copy of the document or **No** to continue in the current document. The selected text is blacked out.



Estimated·turnover·for·2008:· [redacted] ¶

Chapter 4. Protecting Email Attachments

This chapter describes the Workshare Protect functionality with regard to identifying content risk in emails and their attachments. It includes the following sections:

- **Overview – Protecting Email Attachments**, below, introduces how Workshare Protect protects emails.
- **Interactive Protect**, page 32, describes how to use Interactive Protect to secure your emails.
- **Using the Protect Profile Dialog**, page 31, describes how to send secure emails using the Workshare Protect Profile dialog.
- **Using the Email Security Dialog**, page 42, describes how to send secure emails using the Workshare Protect Email Security dialog.
- **Sending Large Files**, page 60, describes how to use the Secure File Transfer functionality to upload large attachments to Workshare Online and send recipients links to the files in Workshare.

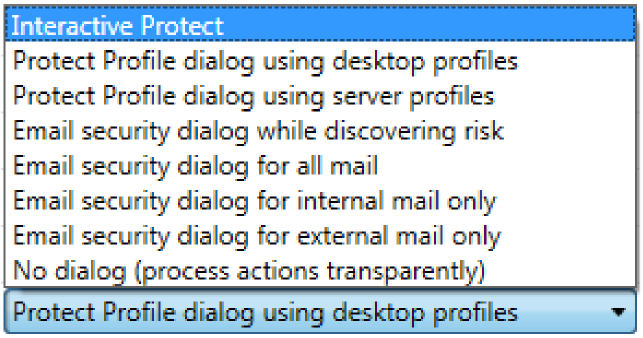
Overview – Protecting Email Attachments

Workshare Protect is able to process the emails you send to ensure security in the following ways:

- Remove metadata from attachments
- Convert attachments to PDF or PDF/A
- Send attachments to a secure location and send recipients a link to that location
- Compress multiple attachments into a single zip file

Whether Workshare Protect processes your emails is determined by the **Apply Workshare Protect** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category). Your administrator may have selected that Workshare Protect processes emails to external recipients only, emails to internal recipients only, all emails or no emails.

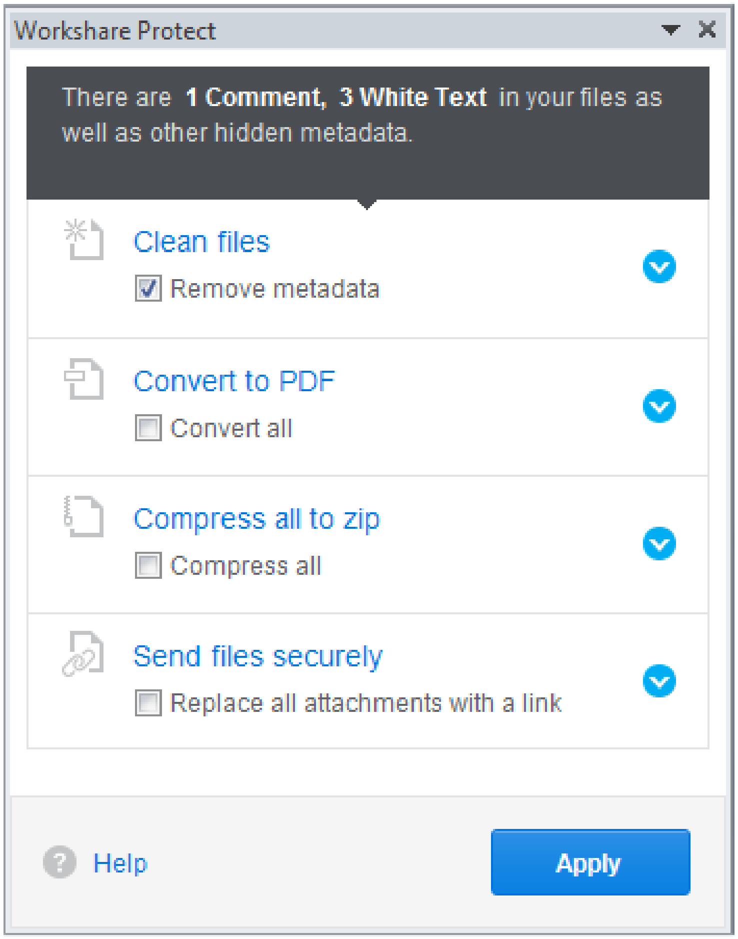
When Workshare Protect is "on", the user experience when sending emails will vary depending on which option your Administrator has selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).


Interactive Protect
Protect Profile dialog using desktop profiles
Protect Profile dialog using server profiles
Email security dialog while discovering risk
Email security dialog for all mail
Email security dialog for internal mail only
Email security dialog for external mail only
No dialog (process actions transparently)
Protect Profile dialog using desktop profiles

When sending emails, you may experience one of the following three options:

- Interactive Protect panel
- Protect Profile dialog
- Email Security dialog

Interactive Protect Panel



Workshare Protect

There are **1 Comment, 3 White Text** in your files as well as other hidden metadata.

Clean files

☑ Remove metadata

Convert to PDF

□ Convert all

Compress all to zip

□ Compress all

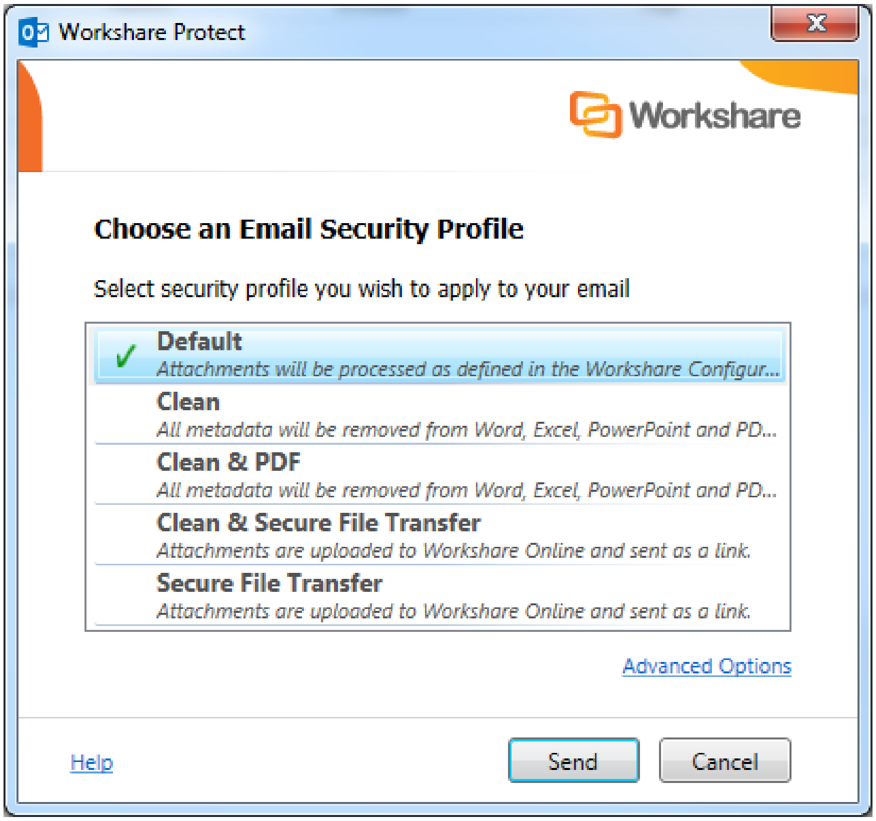
Send files securely

□ Replace all attachments with a link

The Interactive Protect panel is displayed when **Interactive Protect** has been selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).

Interactive Protect is described on page 31.

Protect Profile Dialog



Choose an Email Security Profile

Select security profile you wish to apply to your email

✓ **Default**
Attachments will be processed as defined in the Workshare Configur...

Clean
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & PDF
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

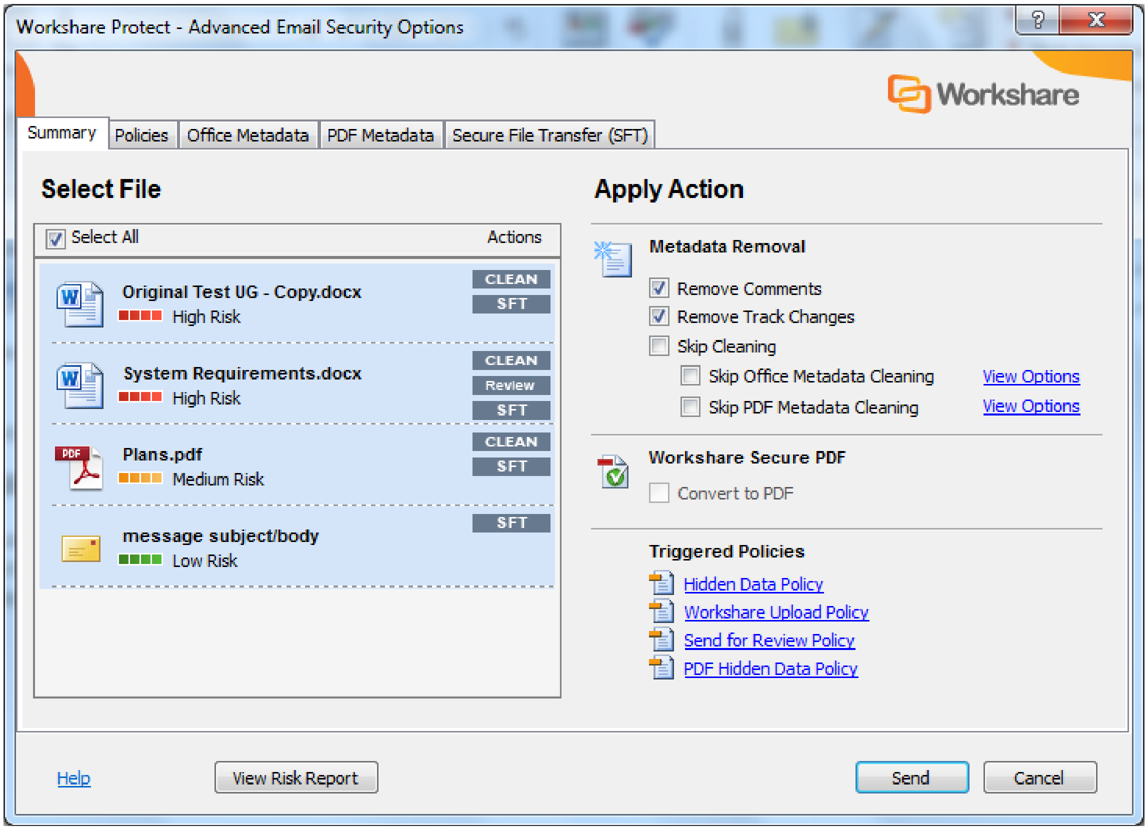
Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

The Protect Profile dialog may be displayed in different ways depending on the option selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).

- **Protect Profile dialog using desktop profiles**: The Protect Profile dialog is displayed after clicking **Send**. It provides a list of profiles available locally from which you can select to apply to your email (shown above).
- **Protect Profile dialog using server profiles**: The Protect Profile dialog is displayed after clicking **Send**. It provides a list of profiles available on Workshare Protect Server from which you can select to apply to your email.

The Protect Profile dialog is described on page 39.

Email Security Dialog



Select File

☑ Select All — Actions

File	Risk	Actions
Original Test UG - Copy.docx	🟥🟥🟥🟥 High Risk	CLEAN SFT
System Requirements.docx	🟥🟥🟥🟥 High Risk	CLEAN Review SFT
Plans.pdf	🟧🟧🟧🟧 Medium Risk	CLEAN SFT
message subject/body	🟩🟩🟩🟩 Low Risk	SFT

Apply Action

Metadata Removal

☑ Remove Comments

☑ Remove Track Changes

□ Skip Cleaning

□ Skip Office Metadata Cleaning — View Options

□ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

□ Convert to PDF

Triggered Policies

- Hidden Data Policy
- Workshare Upload Policy
- Send for Review Policy
- PDF Hidden Data Policy

The Email Security dialog may be displayed in different circumstances depending on the option selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).

- **Email Security dialog while discovering risk**: The *Email Security* dialog is always displayed. It is displayed immediately after clicking **Send** while Workshare Protect checks the email against the default profile. The options are enabled once the check is complete.
- **Email Security dialog for all mail**: The *Email Security* dialog is always displayed. It is displayed after clicking **Send** once Workshare Protect has checked the email against the default profile.
- **Email Security dialog for internal mail only**: The *Email Security* dialog is displayed when an email has internal recipients. It is displayed after clicking **Send** once Workshare Protect has checked the email against the default profile. For email to external recipients only, the *Email Security* dialog is not displayed. This is only relevant when **Apply Workshare Protect** is selected for **Internal Email**.
- **Email Security dialog for external mail only**: The *Email Security* dialog is displayed when an email has external recipients. It is displayed after clicking **Send** once Workshare Protect has checked the email against the default profile. For email to internal recipients only, the *Email Security* dialog is not displayed. This is only relevant when **Apply Workshare Protect** is selected for **External Email**.
- **No dialog (process actions transparently)**: The *Email Security* dialog is not displayed. Workshare Protect processes the email and applies the default profile without any user intervention.

The Email Security dialog is described on page 42.

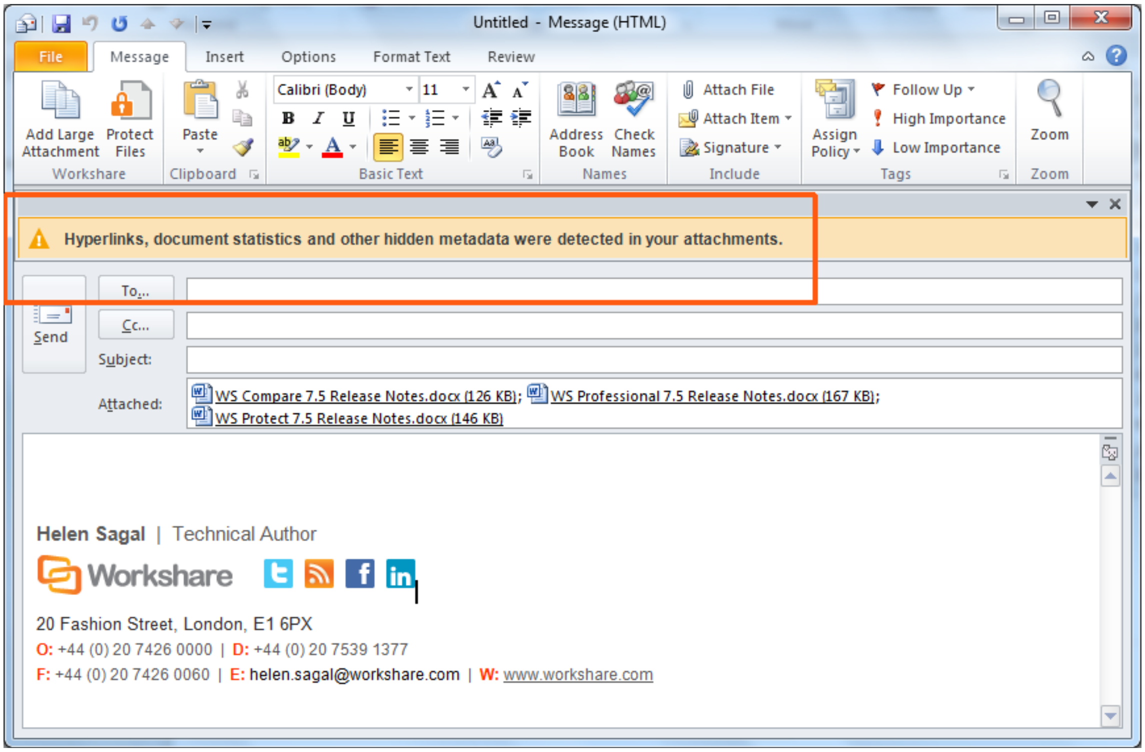
Interactive Protect

The Interactive Protect panel offers you options to control your documents and secure attachments before sending your email.

- **Remove Metadata**: Enables you to clean metadata from your attachments.
- **Convert to PDF**: Enables you to convert all the attachments to PDF or PDF/A.
- **Compress Files**: Enables you to compress all attachments together into one zip file.
- **Secure File Transfer**: Enables you to send your documents to a secure location send recipients a link to that location.

To work with Interactive Protect:

Open Outlook and create a new email. Attach one or more files. Immediately Workshare Protect reports on the metadata found in a notification across the top of your email.



Hyperlinks, document statistics and other hidden metadata were detected in your attachments.

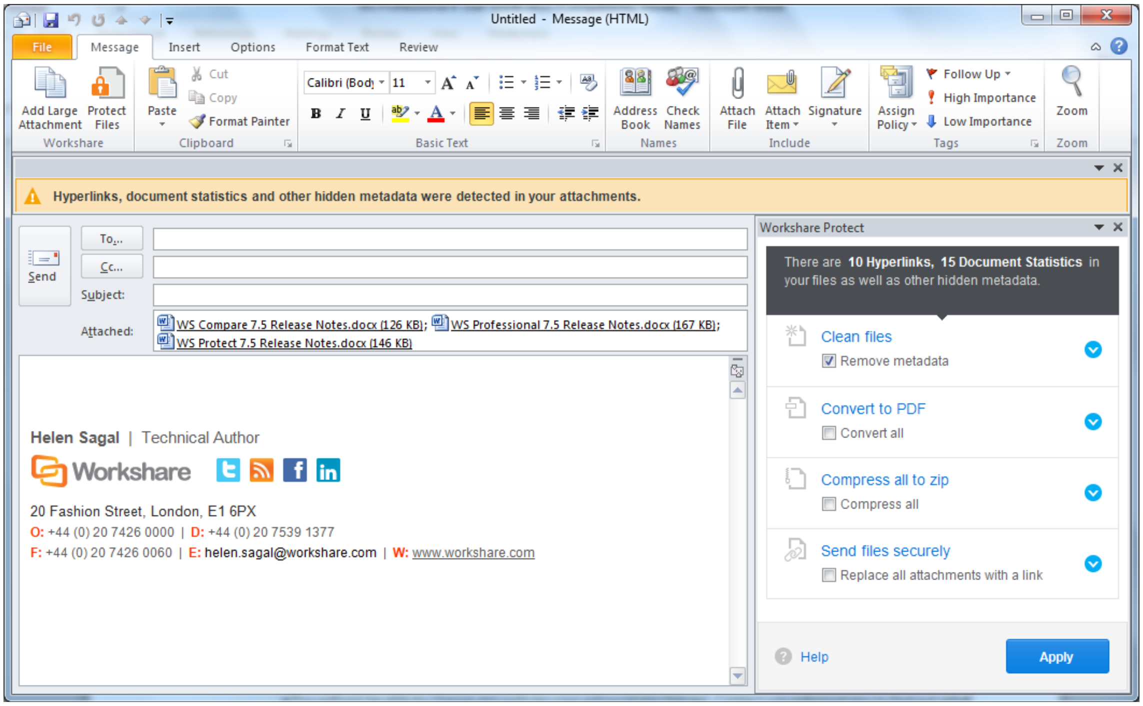
Attached: WS Compare 7.5 Release Notes.docx (126 KB); WS Professional 7.5 Release Notes.docx (167 KB); WS Protect 7.5 Release Notes.docx (146 KB)

Helen Sagal | Technical Author

Workshare

20 Fashion Street, London, E1 6PX
O: +44 (0) 20 7426 0000 | D: +44 (0) 20 7539 1377
F: +44 (0) 20 7426 0060 | E: helen.sagal@workshare.com | W: www.workshare.com

If the Interactive Protect panel doesn't open automatically, click the warning or click **Protect Files** in the Message tab. The Interactive Protect panel is displayed on the right side of your email window.



Untitled - Message (HTML)

⚠ Hyperlinks, document statistics and other hidden metadata were detected in your attachments.

Attached: WS Compare 7.5 Release Notes.docx (126 KB); WS Professional 7.5 Release Notes.docx (167 KB); WS Protect 7.5 Release Notes.docx (146 KB)

Helen Sagal | Technical Author

Workshare

20 Fashion Street, London, E1 6PX
O: +44 (0) 20 7426 0000 | D: +44 (0) 20 7539 1377
F: +44 (0) 20 7426 0060 | E: helen.sagal@workshare.com | W: www.workshare.com

Workshare Protect

There are **10 Hyperlinks, 15 Document Statistics** in your files as well as other hidden metadata.

Clean files
☑ Remove metadata

Convert to PDF
☐ Convert all

Compress all to zip
☐ Compress all

Send files securely
☐ Replace all attachments with a link

Using the options in the panel, you can clean metadata from the attachments, convert them to PDF, compress them in a zip file – all before sending the email. You can preview exactly what the processed attachments will appear like to the recipients BEFORE sending the email. Additionally, you can send the attachments to a secure location in Workshare and send only a link to that location to the recipients.

After selecting the required options, you must click **Apply** and then you can write your email while the changes are being applied before finally clicking **Send** once you are confident that what you are sending is secure and safe.

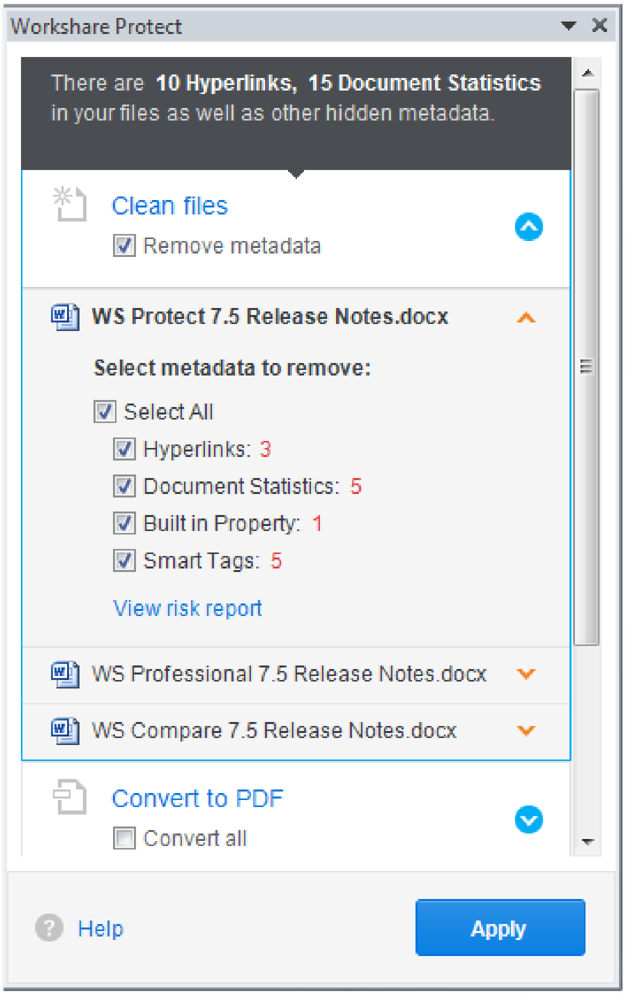
If you do NOT click **Apply** before sending the email, your Interactive Protect settings will not be applied and the attachments will be processed using the default profile.

***Note**: If you create an email with an attachment, clean with Interactive Protect and then close the email, you are not prompted to save the email BUT the email is saved to your drafts folder.*

Cleaning Metadata Using Interactive Protect

In the Interactive Protect panel, you can leave the **Remove metadata** checkbox selected (this is selected by default) and click **Apply**. All metadata is removed from all the attachments.

To select specific metadata to remove from each attachment, you can expand the **Clean files** section.



Workshare Protect

There are **10 Hyperlinks, 15 Document Statistics** in your files as well as other hidden metadata.

Clean files

☑ Remove metadata

WS Protect 7.5 Release Notes.docx

Select metadata to remove:

☑ Select All

☑ Hyperlinks: 3

☑ Document Statistics: 5

☑ Built in Property: 1

☑ Smart Tags: 5

View risk report

WS Professional 7.5 Release Notes.docx

WS Compare 7.5 Release Notes.docx

Convert to PDF

☐ Convert all

You can expand each attachment and adjust the metadata to remove for each one by selecting/deselecting the checkboxes.

***Note**: To view a detailed report of the metadata found in an attachment, click **View risk report**.*

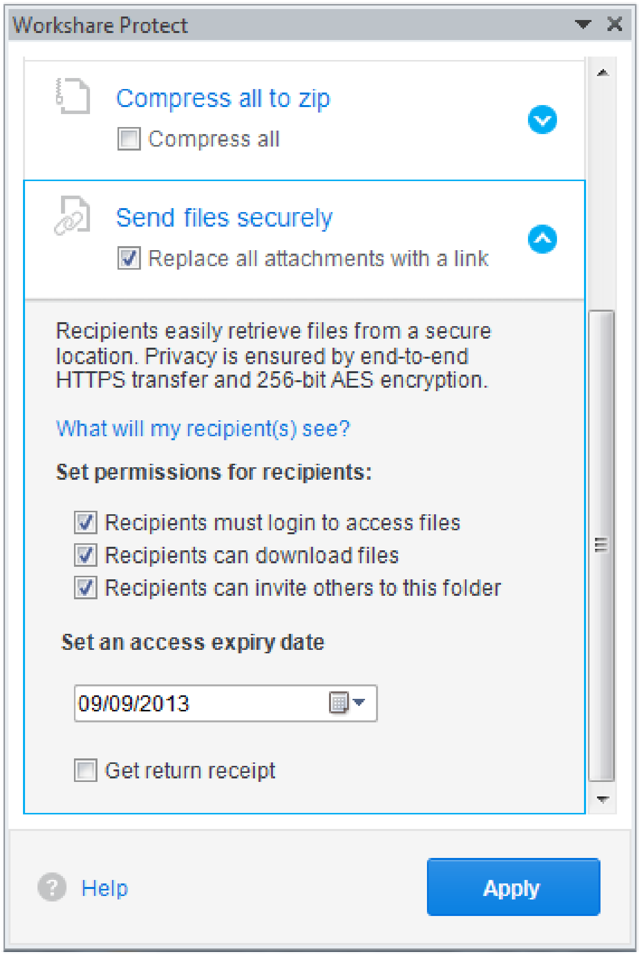
Click **Apply** and the selected metadata is removed from each attachment.

You can write your email while the attachments are being cleaned and then preview the files by opening the cleaned attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

Secure File Transfer Using Interactive Protect

In the Interactive Protect panel, you can select the **Replace all attachments with a link** checkbox selected and click **Apply**. The attachments are uploaded to Workshare Online and are replaced in the email with a link to their secure location.

To change the permissions set for the attachments in Workshare or to set an expiry date, you can select the **Replace all attachments with a link** checkbox and expand the **Send files securely** section.



Workshare Protect

Compress all to zip

☐ Compress all

Send files securely

☑ Replace all attachments with a link

Recipients easily retrieve files from a secure location. Privacy is ensured by end-to-end HTTPS transfer and 256-bit AES encryption.

What will my recipient(s) see?

Set permissions for recipients:

☑ Recipients must login to access files
☑ Recipients can download files
☑ Recipients can invite others to this folder

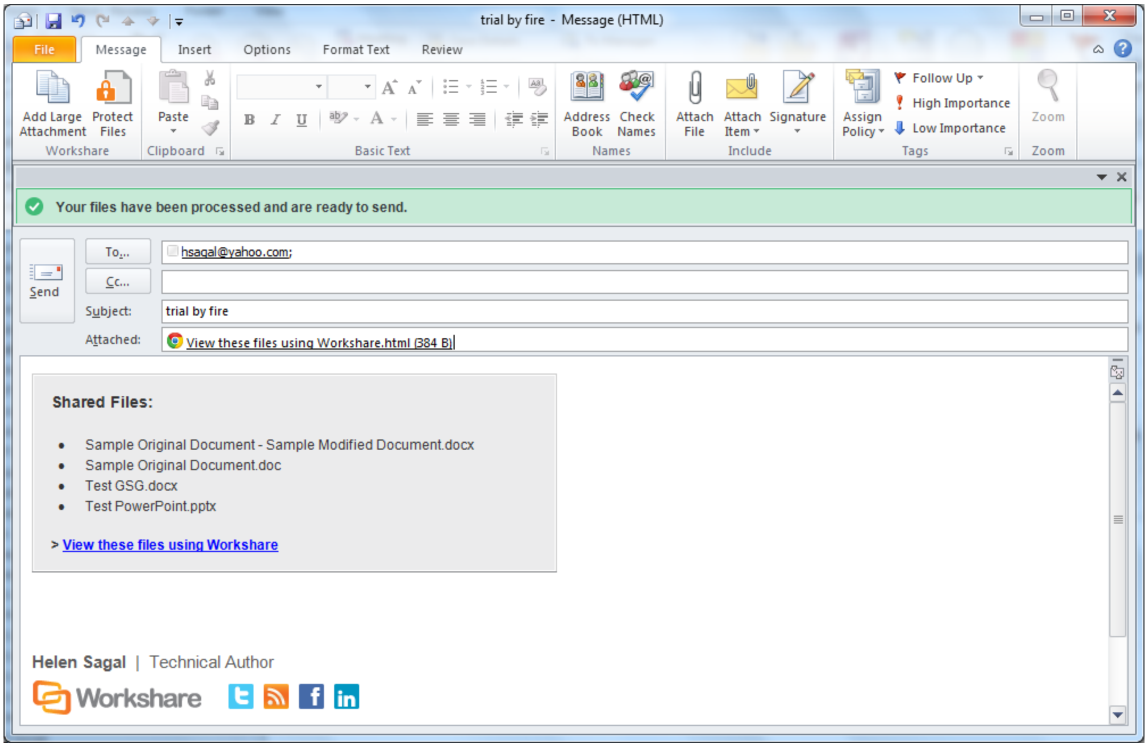
Set an access expiry date

09/09/2013

☐ Get return receipt

- Deselect any of the following permissions for the attachments as required:
  - **Recipients must login to access files**: When selected, the recipient must be a Workshare user and must log into Workshare Online in order to access the files.
  - **Recipients can download files**: When selected, recipients can download the files.
  - **Recipients can invite others to this folder**: When selected, recipients can share the folder where the attachments are stored.
- If required, select an expiry date for the files. After this date, recipients will no longer be able to access the files.
- Select the **Get return receipt** checkbox if you want to receive an email once the recipients have accessed the files.

Click **Apply** and enter your Workshare login credentials in the Workshare Account Details dialog. Click **Log In**. The attachments are uploaded into a single folder in Workshare (named with a date and time stamp) and the attachments are replaced in the email with a link.



Your files have been processed and are ready to send.

To: hsagal@yahoo.com;

Subject: trial by fire

Attached: View these files using Workshare.html (384 B)

Shared Files:

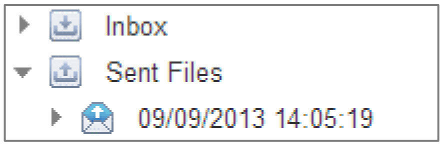
- Sample Original Document - Sample Modified Document.docx
- Sample Original Document.doc
- Test GSG.docx
- Test PowerPoint.pptx

> View these files using Workshare

Helen Sagal | Technical Author

Workshare

You can write your email while the attachments are being processed and then preview the files in Workshare by clicking the link. The files are uploaded into a single folder in your **Sent Items** folder in Workshare and in the Recipients **Inbox** folder.

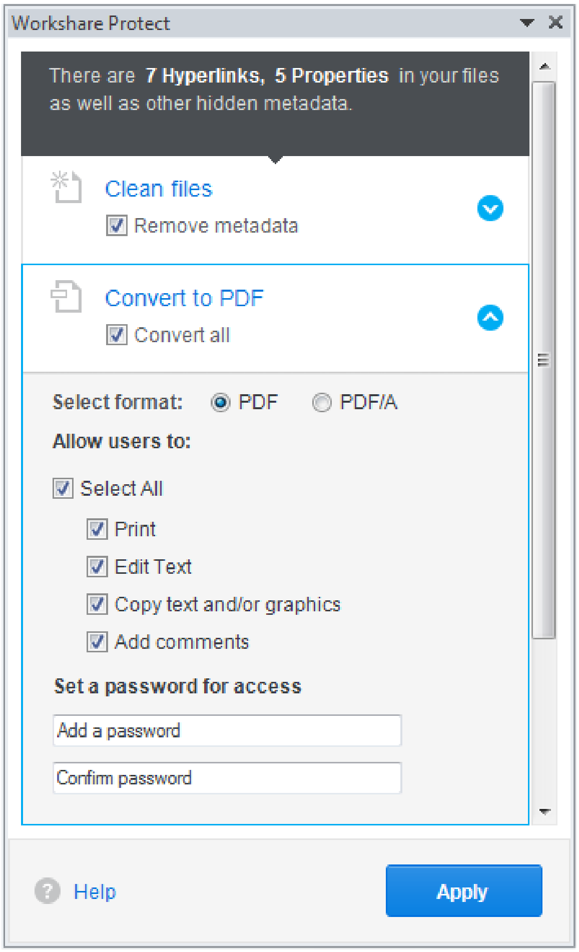


Finally in your email, click **Send** once you are confident that what you are sending is secure and safe.

Converting Attachments to PDF Using Interactive Protect

In the Interactive Protect panel, you can select the **Convert all** checkbox in the **Convert to PDF** section and click **Apply** and all attachments are converted to PDF.

To select specific PDF conversion settings for the attachments, you can select the **Convert all** checkbox and expand the **Convert to PDF** section.



Workshare Protect

There are **7 Hyperlinks, 5 Properties** in your files as well as other hidden metadata.

Clean files

☑ Remove metadata

Convert to PDF

☑ Convert all

Select format: ● PDF ○ PDF/A

Allow users to:

☑ Select All

- ☑ Print
- ☑ Edit Text
- ☑ Copy text and/or graphics
- ☑ Add comments

Set a password for access

Add a password

Confirm password

- Select whether to convert the attachments to PDF or PDF/A.
- Select all or some of the following security options:
  - **Print:** Prevents recipients from printing PDF files.
  - **Edit Text:** Prevents recipients with Adobe Distiller from editing PDF files.
  - **Copy text and/or graphics:** Prevents recipients from copying graphics or text directly from PDF files.
  - **Add comments:** Prevents recipients with Adobe Distiller from adding comments to PDF files.

> ***Note:*** *These options are not available if you selected PDF/A.*

- If required, set a password to protect the PDF files by entering the password twice. When a password is specified, recipients can only open the PDF files after entering this password.

> ***Note:*** *This option is not available if you selected PDF/A.*

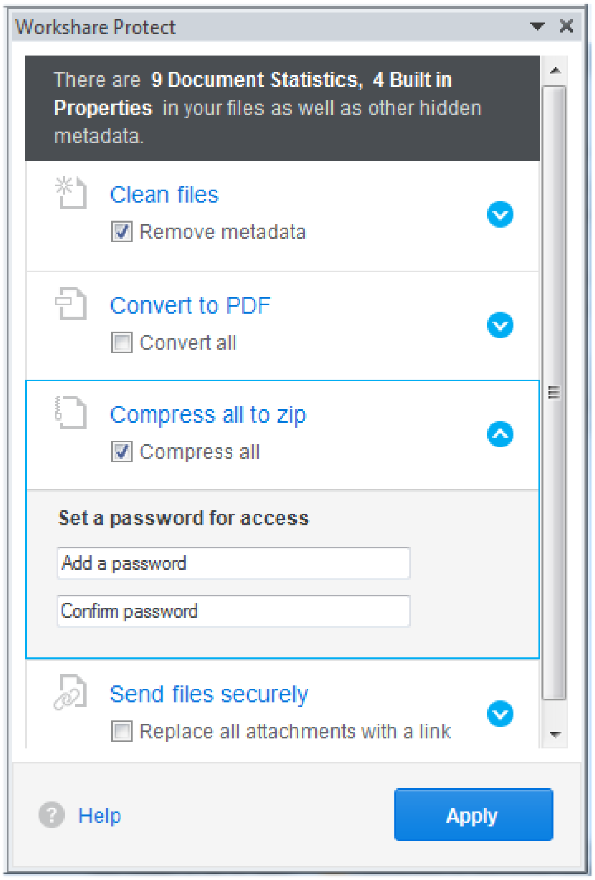
Click **Apply** and the selected PDF settings are applied to all attachments.

You can write your email while the attachments are being converted and then preview the files by opening the converted attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

Compressing Attachments Using Interactive Protect

In the Interactive Protect panel, you can select the **Compress all** checkbox in the **Compress all to zip** section and click **Apply** and all attachments are converted to PDF.

To set a password for the zip file, you can select the **Compress all** checkbox and expand the **Compress all to zip** section.



Workshare Protect

There are **9 Document Statistics, 4 Built in Properties** in your files as well as other hidden metadata.

Clean files

☑ Remove metadata

Convert to PDF

☐ Convert all

Compress all to zip

☑ Compress all

Set a password for access

Add a password

Confirm password

Send files securely

☐ Replace all attachments with a link

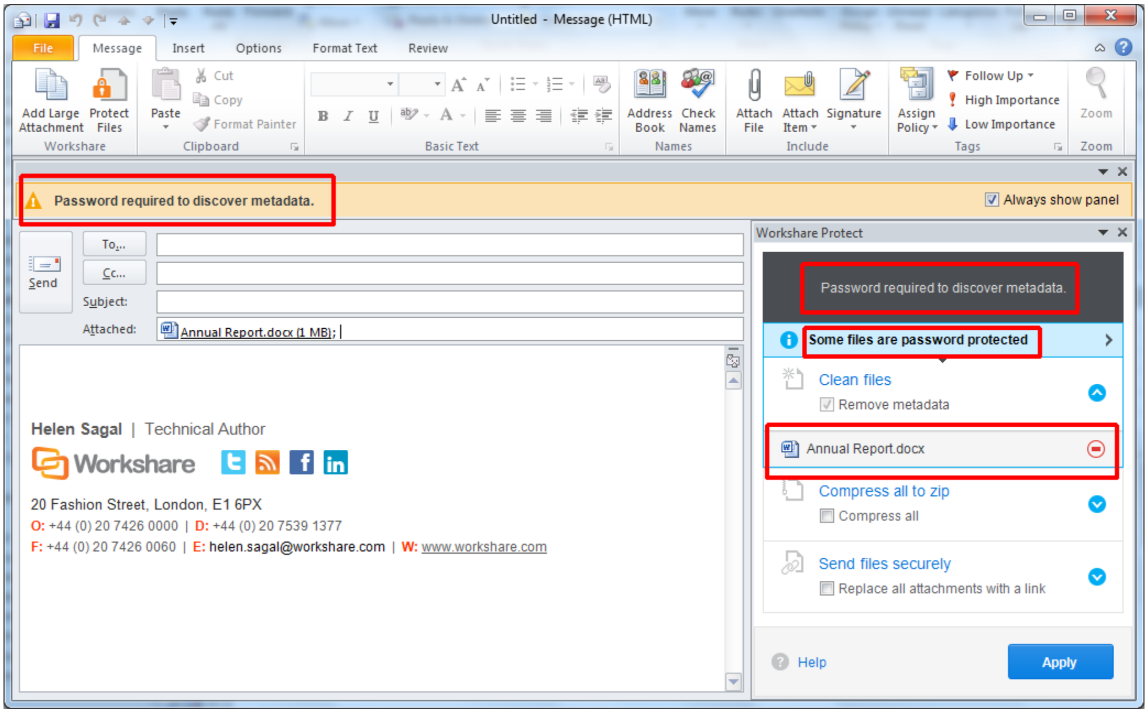
If required, set a password to protect the zip file by entering the password twice. When a password is specified, recipients can only open the zip file after entering this password.

Click **Apply** and all the attachments are compressed into a single zip file called **Attachments.zip**.

You can write your email while the attachments are being compressed and then preview the files by opening the zip attachment. Finally click **Send** once you are confident that what you are sending is secure and safe.

Password Protected Files and Interactive Protect

When you attach a password-protected file, Workshare cannot clean or convert the file unless you enter the password. Warnings are shown in your email window as follows:



Password required to discover metadata.

☑ Always show panel

Subject:

Attached: Annual Report.docx (1 MB);

Helen Sagal | Technical Author

Workshare

20 Fashion Street, London, E1 6PX
O: +44 (0) 20 7426 0000 | D: +44 (0) 20 7539 1377
F: +44 (0) 20 7426 0060 | E: helen.sagal@workshare.com | W: www.workshare.com

Workshare Protect

Password required to discover metadata.

Some files are password protected

Clean files
☑ Remove metadata

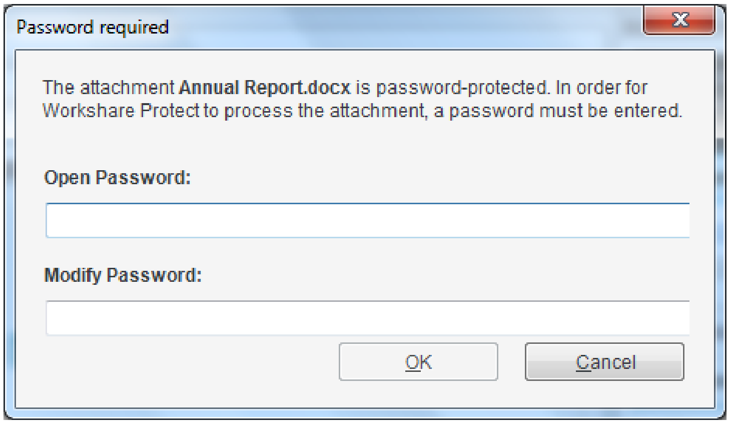
Annual Report.docx

Compress all to zip
☐ Compress all

Send files securely
☐ Replace all attachments with a link

In order to proceed and clean the attachment or convert it to PDF, you must enter the open/modify password.

Click the ⊖ icon. The Password required dialog is displayed.


Password required

The attachment **Annual Report.docx** is password-protected. In order for Workshare Protect to process the attachment, a password must be entered.

Open Password:

Modify Password:

Enter the Open or Modify passwords (or both) and click **OK**.

You will now be able to expand the attachment in the Interactive Protect panel and select which metadata to remove or whether to convert the attachment to PDF.

> ***Note**: You can send password-protected attachments securely and compress them without the need to enter the open/modify password.*

Using the Protect Profile Dialog

The *Protect Profile* dialog provides a simple UI that enables you to select what profile to apply to your emails.

A profile is a collection of policies that include a set of instructions to Workshare Protect as to what metadata to remove from an email attachment, whether to convert the attachment to PDF and whether to upload the attachment to Workshare Online and send a link instead.

Metadata settings and PDF instructions are specified per file type – Microsoft Word documents, Excel spreadsheets and PowerPoint presentations as well as PDF files. So for example, a profile could specify that comments and hidden text should be removed from Microsoft Word attachments and the document should be converted to PDF and only hidden worksheets should be removed from Microsoft Excel attachments and they should not be converted to PDF.

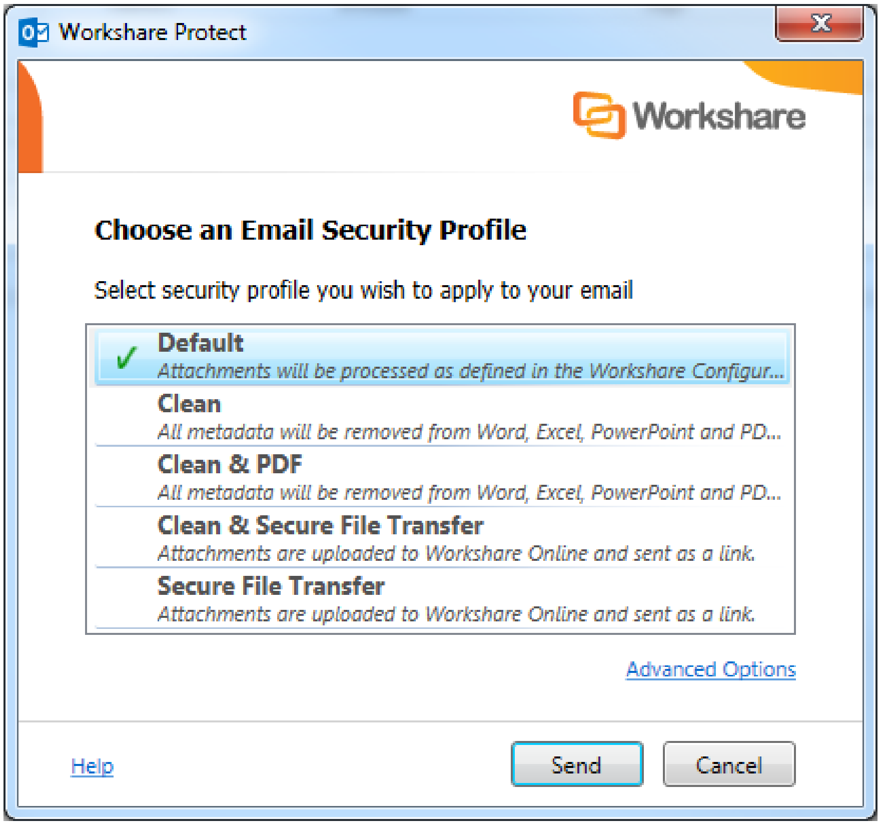
Your administrator defines profiles. Your administrator may have adopted a task-based approach or recipient-based approach when creating profiles:

- **Task-based profiles**: For example, you are working on a legal document and sending it to colleagues to receive input. You email it and select the "Working Draft" profile which will remove metadata but keep track changes and comments. After receiving input and implementing changes, you email it and select the "Final Draft" profile which will remove metadata and remove track changes and comments. Once you are happy with the document, you email it and select the "Final" profile which will remove metadata, track changes and comments and convert the document to PDF.
- **Recipient-based profiles**: For example, your company has a policy that whatever documents you send to opposing counsel, the metadata must be removed and the document must be converted to PDF. You therefore have a profile called "opposing counsel" which removes metadata and converts to PDF. You also have a profile called "Personal" which does nothing.

These are just examples of the types of profiles that might be defined. If you have any questions or requirements regarding the profiles, contact your administrator.

To send an email:

1. Create a new email, attach the required document(s) and click **Send**. The *Protect Profile* dialog is displayed.



Workshare Protect

Choose an Email Security Profile

Select security profile you wish to apply to your email

✓ **Default**
Attachments will be processed as defined in the Workshare Configur...

Clean
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & PDF
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

2. Select the profile you want to apply to your attachments and click **Send**. The following default profiles are provided with Workshare Protect:
   - **Default**: Attachments are processed according to the settings in the Workshare Configuration Manager.
   - **Clean**: All metadata is cleaned from Microsoft Word, Excel, PowerPoint and PDF attachments.
   - **Clean & PDF**: All metadata is cleaned from Microsoft Word, Excel, PowerPoint and PDF attachments and Microsoft Word, Excel and PowerPoint attachments are also converted to PDF.
   - **Clean & Secure File Transfer**: All metadata is cleaned from Microsoft Word, Excel, PowerPoint and PDF attachments and then the attachments are uploaded to Workshare Online and recipients are sent a link to the attachments. Refer to *Secure File Transfer Profiles*, page 42.
   - **Secure File Transfer**: Attachments are uploaded to Workshare Online and recipients are sent a link to the attachments. Refer to *Secure File Transfer Profiles*, page 42.

If you want to send your email without Workshare Protect processing the attachments, click the arrow on the **Send** button and select **Send without processing**.

If you want to access *the Email Security* dialog and specify personal settings or individual settings for each attachment, click the **Advanced Options** link. The *Email Security* dialog is displayed with options matching the profile selected. Refer to the next section for a description of the *Email Security* dialog.

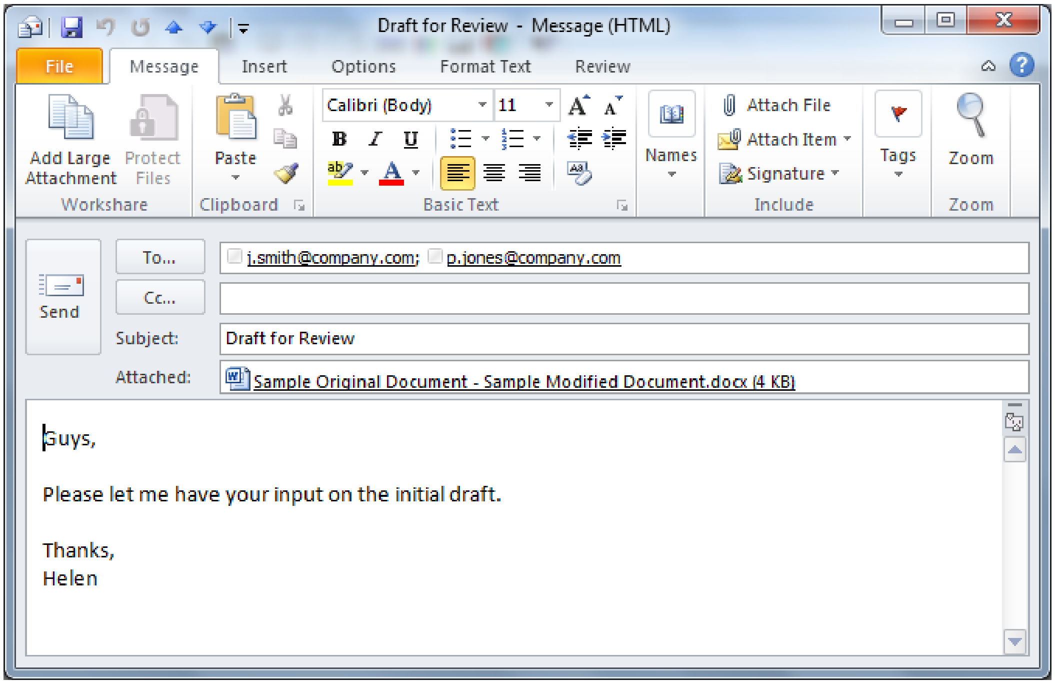
***Note**: Your administrator may not have enabled the Secure File Transfer profiles or the **Send without processing** option or the **Advanced Options** link.*

Secure File Transfer Profiles

You can upload almost any file to Workshare Online and send any recipient a link to where the document is stored in Workshare. All recipients will be able to view the document in Workshare in a browser and those recipients who have a Workshare account will also be able to collaborate on the documents by adding comments in real-time and uploading versions.

To securely transfer files:

1. Create a new email, enter the recipient email addresses and attach the required document(s).



To: j.smith@company.com; p.jones@company.com

Subject: Draft for Review

Attached: Sample Original Document - Sample Modified Document.docx (4 KB)

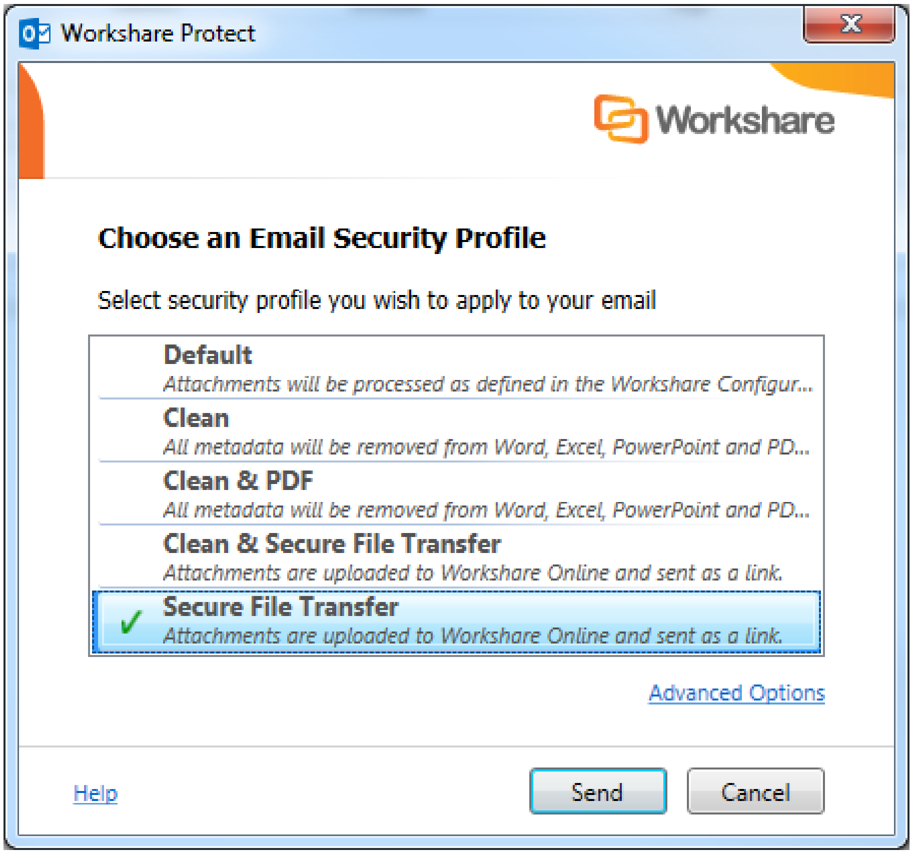
Guys,

Please let me have your input on the initial draft.

Thanks,
Helen

2. Click **Send**. The *Protect Profile* dialog is displayed.

3. Select **Secure File Transfer** or **Clean & Secure File Transfer** (if you want to remove metadata from the attachments before uploading them to Workshare).



Choose an Email Security Profile

Select security profile you wish to apply to your email

Default
Attachments will be processed as defined in the Workshare Configur...

Clean
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & PDF
All metadata will be removed from Word, Excel, PowerPoint and PD...

Clean & Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

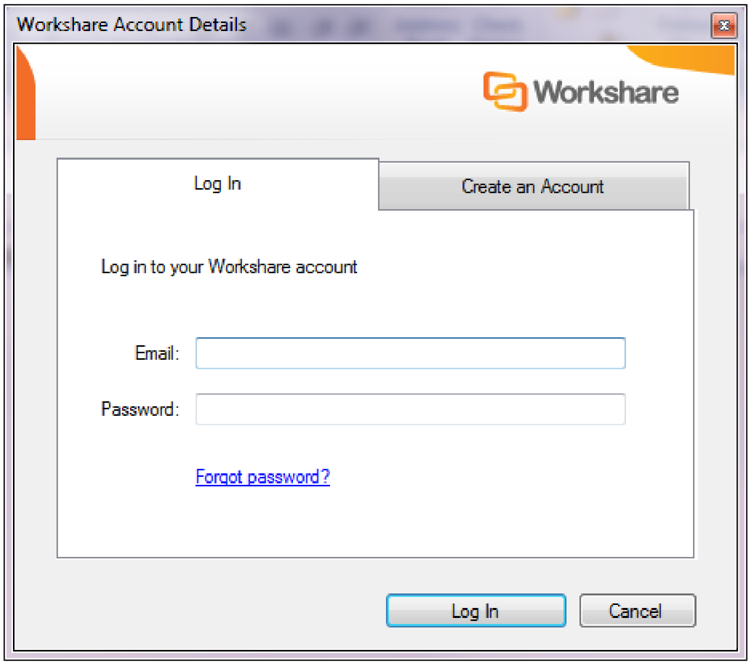
✓ **Secure File Transfer**
Attachments are uploaded to Workshare Online and sent as a link.

> ***Note***: *Click **Advanced Options** if you want to configure specific user access to the documents in Workshare. Refer to Advanced Options, page 45.*

4. Click **Send**. The *Workshare Account Details* dialog is displayed.

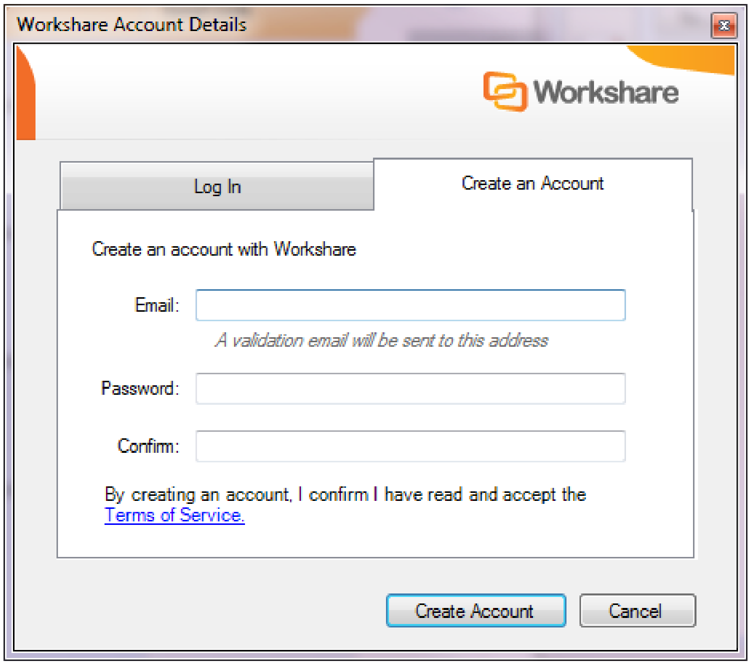
> ***Note***: *If you are already logged into Workshare, the attached files are uploaded to a folder in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time.*

- If you already have an account with Workshare, in the **Log In** tab, enter your Workshare login email and password and click **Log In**. The attached files are uploaded to a folder in Workshare.



Log in to your Workshare account

- If you are new to Workshare, complete the **Create an account** tab by entering an email address and password to use as your Workshare login.



Create an account with Workshare

A validation email will be sent to this address

By creating an account, I confirm I have read and accept the Terms of Service.

Click **Create Account**. A message indicating that you must validate your new account is displayed. Click **OK**. The email is sent but the recipient will not be able to access the attachment until you have validated your account. Open the validation email and click the link in that email to validate your account.

The attached files are uploaded to a folder in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time. This folder appears in your **Sent Items** folder in My Files and Folders in Workshare. The recipient receives an email notifying them that files have been uploaded to Workshare and providing a link to the files.

Receiving Links

Recipients of emails sent using the Secure File Transfer profiles receive an email with details of the name of the file and a link to click to access the file in Workshare Online. The means of access and options available to the recipient will vary depending on whether the recipient is a Workshare user and the settings specified by the sender. Scenarios include:

- When a recipient is a Workshare user, clicking the link displays the location in Workshare where the file (or files) is stored. The file or files are stored in a folder with a name that matches the subject of the email. This folder appears in the recipient's **Inbox** folder in My Files and Folders in Workshare. The recipient can add comments to the file, upload versions and make changes to the folder where the file is stored.
- If the sender has specified that the recipient need not be a Workshare user, clicking the link displays the location in Workshare where the file (or files) is stored. The recipient can view the file and download it.
- If the sender has specified that the recipient must be logged in to Workshare, clicking the link displays the Workshare login and the recipient must first log in to Workshare in order to view the location in Workshare where the file (or files) is stored and download it.
- If the sender has specified an expiry date then the link will only work until the expiry date. Once the date has passed, the recipient will not be able to access the file.

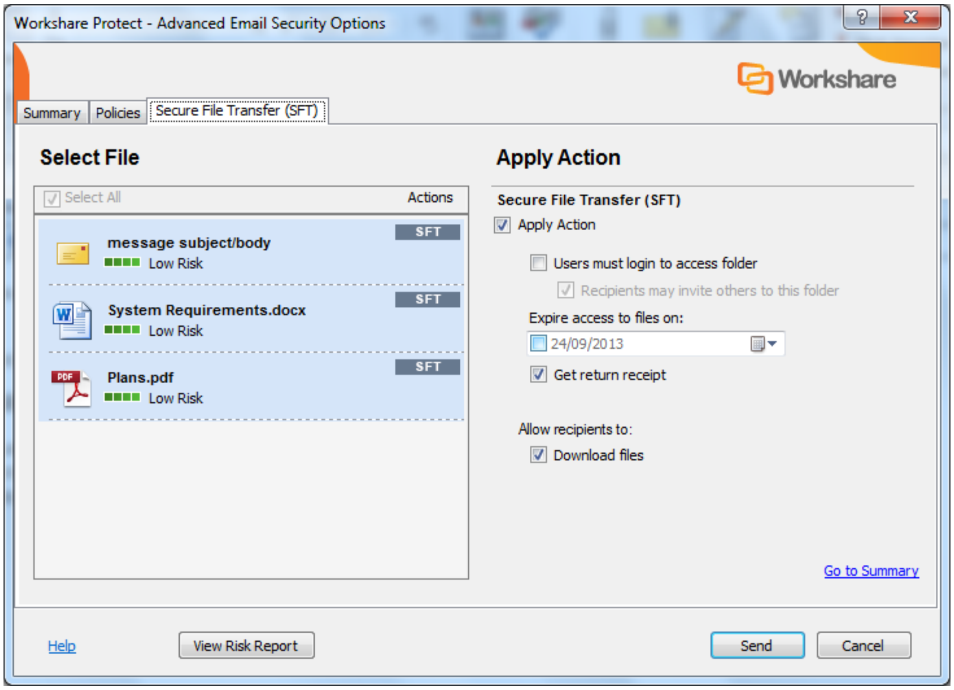
Advanced Options

You can set advanced access rights to documents that you store in Workshare to control recipient access. Clicking **Advanced Options** in the *Protect Profile* dialog enables you to configure specific user access to the documents you are uploading to Workshare.

To configure advanced options:

1. Create a new email, enter the recipient email addresses and attach the required document(s).
2. Click **Send**. The *Protect Profile* dialog is displayed.
3. Select **Secure File Transfer** or **Clean & Secure File Transfer** and click **Advanced Options**. The *Advanced Email Security Options* dialog is displayed.

4. Select the **Secure File Transfer (SFT)** tab.



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All | Actions

message subject/body Low Risk	SFT
System Requirements.docx Low Risk	SFT
Plans.pdf Low Risk	SFT

Apply Action

Secure File Transfer (SFT)

☑ Apply Action

□ Users must login to access folder

☑ Recipients may invite others to this folder

Expire access to files on:

□ 24/09/2013

☑ Get return receipt

Allow recipients to:

☑ Download files

5. If your administrator has given you the rights to access the Advanced Options, you can configure the following parameters:

Apply Action When selected the selected profile (**Secure File Transfer** or **Clean & Secure File Transfer**) is applied to the email. When not selected, the email is sent without a profile being applied.

Users must login to access folder When selected, the recipient must be a Workshare user and must log into Workshare in order to access the file. When not selected, the recipient can access Workshare without being a registered user to view and download the file only.

Recipients may invite others to this folder When selected, recipients can forward the link to other recipients who will be able to access the file. Unless **Users must login to access folder** is selected, this option is always selected.

Expire access to files on: You can specify an expiry date for the file. After this date, the recipient will no longer be able to access the file.

Get return receipt When selected, you will receive an email once the recipient has accessed the file.

Download files When selected, recipients can download the file.

***Note**: The default settings of these parameters are set in the Workshare Policy Designer.*

6. You specify these settings for the files selected on the left side. So you can select multiple files and set the same settings for all or you can select an individual file and specify setting individually.

7. Click **Send**. The attached files are uploaded to a folder in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time.

Using the Email Security Dialog

When you send an email using the *Email Security* dialog configuration, Workshare Protect checks any attachments to see if they breach any security policies defined in the default profile. A security policy defines the conditions that must exist in order for Workshare Protect to detect content risk and the actions that should be taken when the conditions are met (i.e. content risk is found).

When deciding which policy to apply, Workshare Protect checks each recipient. If an external recipient is found, external policy settings are applied. Only if all recipients are internal, are internal policy settings applied. For example, an attached document could contain hidden data that should not be sent to external parties but is suitable for distribution internally.

The options available to you depend on the security policies in place in your organization and the action specified for a policy breach. The different actions are as follows:

- **Block Action**: This action blocks your attempts to send the email until the offending information is removed. See Resolving Blocked Emails for more information.
- **Alert Action**: This action alerts you to content risk contained within your email, although you are still able to send the email. See Reviewing Alerts for more information.
- **Clean Action/Lightspeed Clean Action/PDF Clean**: This action cleans the attachments before sending the email. See Cleaning Hidden Data from Attachments for more information.
- **PDF Action**: This action converts attached documents to PDF before sending the email. See Converting Attachments to PDF for more information.

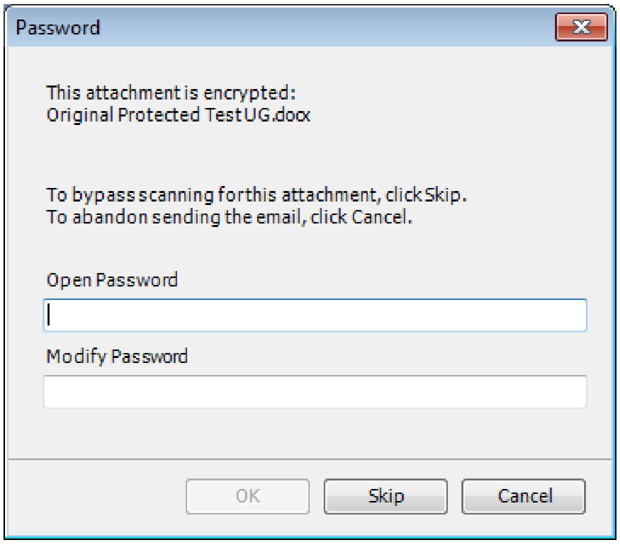
Note: *Using the* ***Apply Workshare Protect*** *parameter in the Workshare Configuration Manager (****Protection*** *>* ***Administration*** *category), Workshare Protect can be configured to NOT check attachments of emails sent internally or externally (or both) to see if they breach any security policies. If you have queries about your email security settings, refer to your administrator.*

Password-Protected Documents

When an attachment is encrypted (password-protected), Workshare Protect requires the password in order to check the document. Password-protection here refers to the file encryption functionality available in MS Word where the user can set a password that must be entered in order to **open** or **modify** the document.

Note*: This functionality is available by clicking the File menu/Office button, selecting* ***Save As*** *and from the Save As dialog, clicking* ***Tools*** *and then selecting* ***General Options****.*

When sending an email with an attachment that requires a password in order to be opened or modified, a *Password* dialog is displayed. For example,



This attachment is encrypted:
Original Protected Test UG.docx

To bypass scanning for this attachment, click Skip.
To abandon sending the email, click Cancel.

Open Password

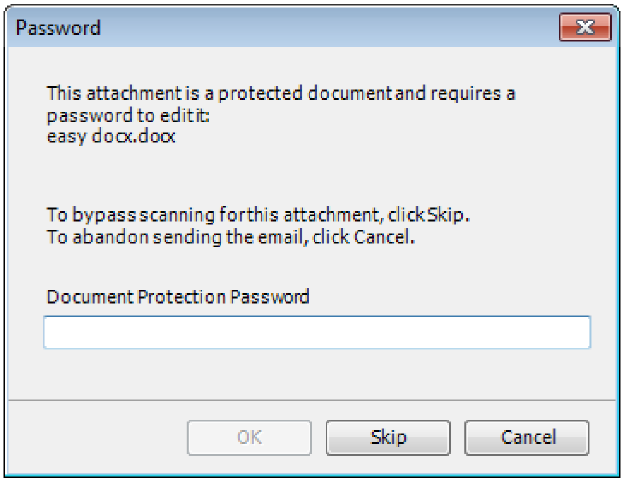
Modify Password

Enter the password required to open the document in the **Open Password** or **Modify Password** field and click **OK**, or you can click **Skip** and Workshare Protect will not check the document.

When an attachment is a protected document, Workshare Protect also requires the password in order to check the document. Protected document refers to the "Protect Document" functionality available in MS Word where the user can restrict specific users from editing specific sections of the document. The protection settings are protected by a password.

> ***Note**: This functionality is available from the **Review** tab (**Protect** group) – click **Restrict Editing** (MS Word 2010/2013) or click **Protect Document** (MS Word 2007).*

When sending an email with an attachment that is a protected document, a *Password* dialog is displayed. For example,



This attachment is a protected document and requires a password to edit it:
easy docx.docx

To bypass scanning for this attachment, click Skip.
To abandon sending the email, click Cancel.

Document Protection Password

Enter the password required to open the document in the **Document Protection Password** field and click **OK**, or you can click **Skip** and Workshare Protect will not check the document.

Send and Protect

Your administrator may have configured Workshare Protect to include a **Send and Protect** button in your message window. If so, you can click this button instead of clicking **Send** and the *Email Security* dialog will always be displayed – regardless of policy settings. You can then select to clean attachments or convert attachments to PDF as required.

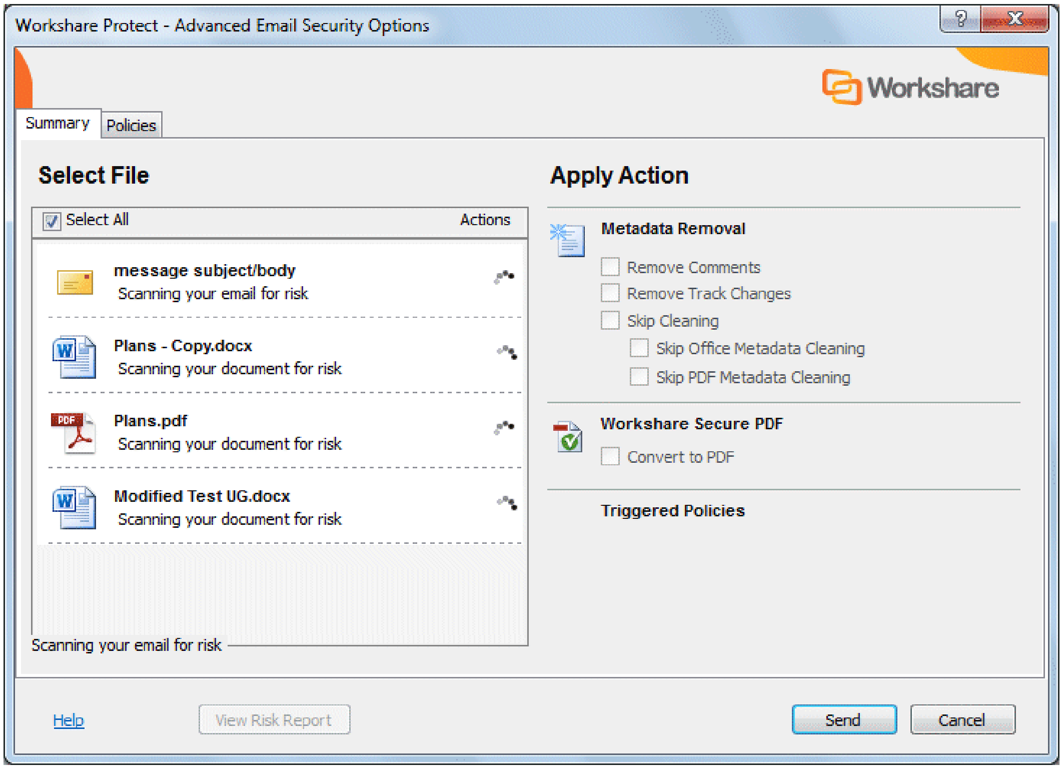
Sending Emails

The following procedure describes how to send emails using the *Email Security* dialog.

To send an email:

Create a new email, attach the required document(s) and click **Send**. The *Email Security* dialog is displayed.

> ***Note****: If the* ***Email Security dialog while discovering risk*** *option has been selected (****When sending an email with attachments show*** *parameter,* ***Protection*** *>* ***Administration*** *category), the Email Security dialog is displayed immediately while Workshare Protect checks the email against the default profile. The options are enabled once the check is complete (see example screen below). When this option is not selected, a progress bar is first displayed and the Email Security dialog is only displayed once the check is complete.*



Workshare Protect - Advanced Email Security Options

Workshare

Summary | Policies

Select File

☑ Select All — Actions

message subject/body
Scanning your email for risk

Plans - Copy.docx
Scanning your document for risk

Plans.pdf
Scanning your document for risk

Modified Test UG.docx
Scanning your document for risk

Scanning your email for risk

Apply Action

Metadata Removal

- □ Remove Comments
- □ Remove Track Changes
- □ Skip Cleaning
  - □ Skip Office Metadata Cleaning
  - □ Skip PDF Metadata Cleaning

Workshare Secure PDF

- □ Convert to PDF

Triggered Policies

This dialog alerts you to any breaches of security policies in the default profile triggered by your email or its attachments. If your administrator has given you permissions, you can modify the settings for each attachment. Refer to Quick Tour of the Email Security Dialog for further information about the options available.

If the **Email Security dialog while discovering risk** option has been selected and you click **Send** before Workshare Protect has finished checking the email, the email is sent and the attachment(s) is processed according the settings in the default profile. This mean that the actual metadata that is cleaned and the settings used for converting to PDF are taken from the default profile.

Click **Send** and Workshare Protect processes the email as specified.

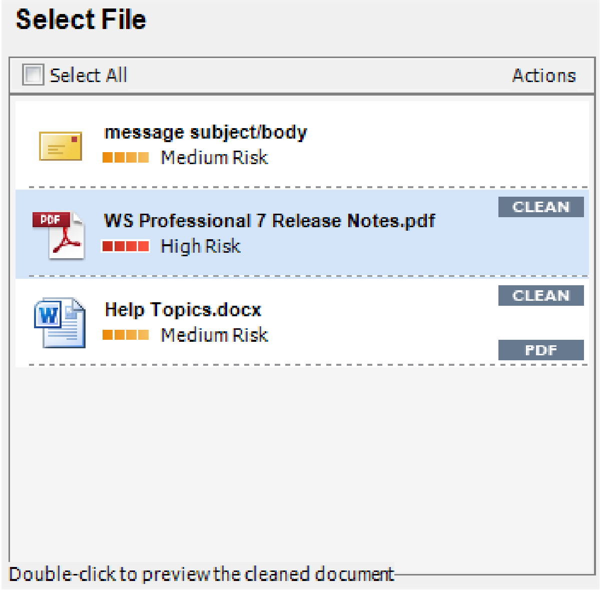
Quick Tour of the Email Security Dialog

The *Email Security* dialog includes several tabs. The number of tabs may vary according to the policies triggered but there will always be a **Summary** tab and a **Policies** tab.

> ***Tip!*** *Click* ***View Risk Report*** *if you want to print a risk report detailing the content risk discovered in the attached document(s). The risk report enables you to evaluate the content risk contained in the selected attachments.*

Select File Area

The **Select File** area is the same in every tab. It includes a list of the email attachments that have triggered a policy.


Select File

☐ Select All

Actions

message subject/body
Medium Risk

WS Professional 7 Release Notes.pdf
High Risk

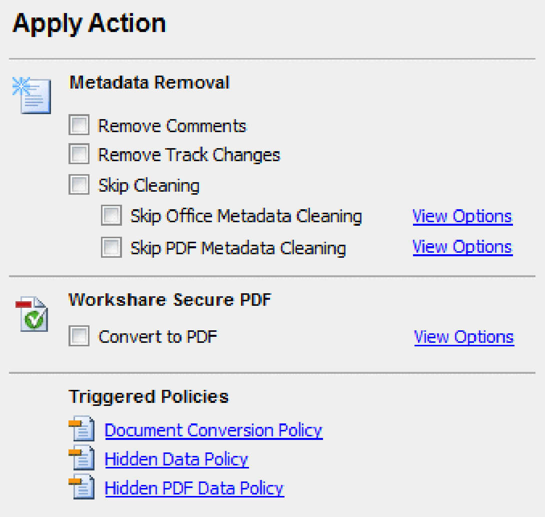
Help Topics.docx
Medium Risk

Double-click to preview the cleaned document

For each item, you can see the risk level and the actions to be applied to the item. You can select individual attachments or select the entire list by selecting the **Select All** checkbox. When a Clean or PDF action is to be applied, you can double-click an item in the list to preview what it will look like once the actions have been applied. For example, if an attachment in DOC format will have the PDF action applied, double-clicking this DOC attachment will enable you to preview it as a PDF.

Summary Tab

The **Apply Action** area of the **Summary** tab provides one-click checkboxes to change details of the Clean and PDF actions as well as a list of triggered policies which provides links to the policies that triggered the actions.



Apply Action

Metadata Removal

□ Remove Comments
□ Remove Track Changes
□ Skip Cleaning
□ Skip Office Metadata Cleaning — View Options
□ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

□ Convert to PDF — View Options

Triggered Policies

- Document Conversion Policy
- Hidden Data Policy
- Hidden PDF Data Policy

Under **Metadata Removal**, selecting **Remove Comments** or **Remove Track Changes** cleans comments or track changes from the selected attachment. Selecting one of the **Skip Cleaning** options means the selected attachment is not cleaned at all. Click **View Options** to display all options in the **Office Metadata/PDF Metadata** tabs.

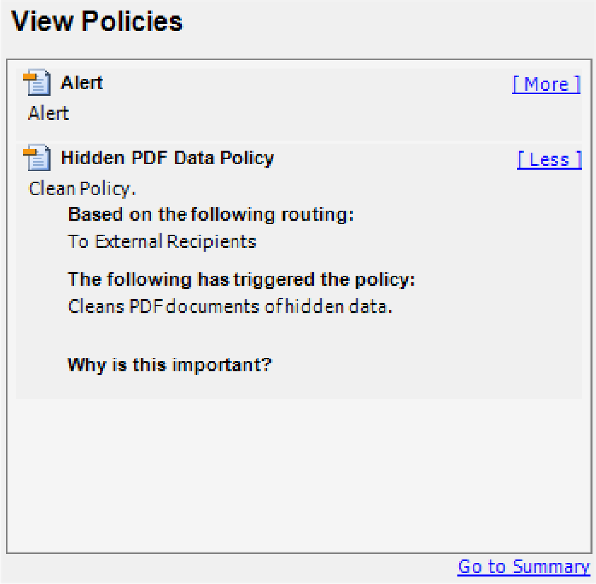
Under **Workshare Secure PDF**, selecting **Convert to PDF** means the selected attachment is converted into PDF. Click **View Options** to display all options in the **Convert to PDF** tab.

Under **Triggered Policies**, there is a list of policies triggered by the email and its attachments. Click the name of a policy to see more information about the policy in the **Policies** tab.

> ***Note:*** *The availability of checkboxes and options may appear differently depending on your organization's security policies included in the default profile. Any options that are disabled have been locked. Refer to your system administrator if you need to override these settings.*

Policies Tab

The **View Policies** area on the right side of the **Policies** tab provides detailed information about the policies breached by the email and it attachments.



View Policies

Alert [More]
Alert

Hidden PDF Data Policy [Less]
Clean Policy.
Based on the following routing:
To External Recipients
The following has triggered the policy:
Cleans PDF documents of hidden data.

Why is this important?

Go to Summary

In the **Policies** tab, you can discover more information about what caused a breach of policy. Click **More**/**Less** to display/hide details of each policy as required.

Other Tabs

The **Office Metadata** tab is included in the *Email Security* dialog when a Clean or Lightspeed Clean action is triggered for an Office file. Refer to *Cleaning Hidden Data from Attachments*, page 55, for more information.

The **PDF Metadata** tab is included in the *Email Security* dialog when a PDF Clean action is triggered for a PDF file. Refer to *Cleaning Hidden Data from Attachments*, page 55, for more information.

The **Convert to PDF** tab is included in the *Email Security* dialog when a PDF action is triggered. Refer to *Converting Attachments to PDF*, page 58, for more information.

The **ZIP Options** tab is included in the *Email Security* dialog when a Zip action is triggered.

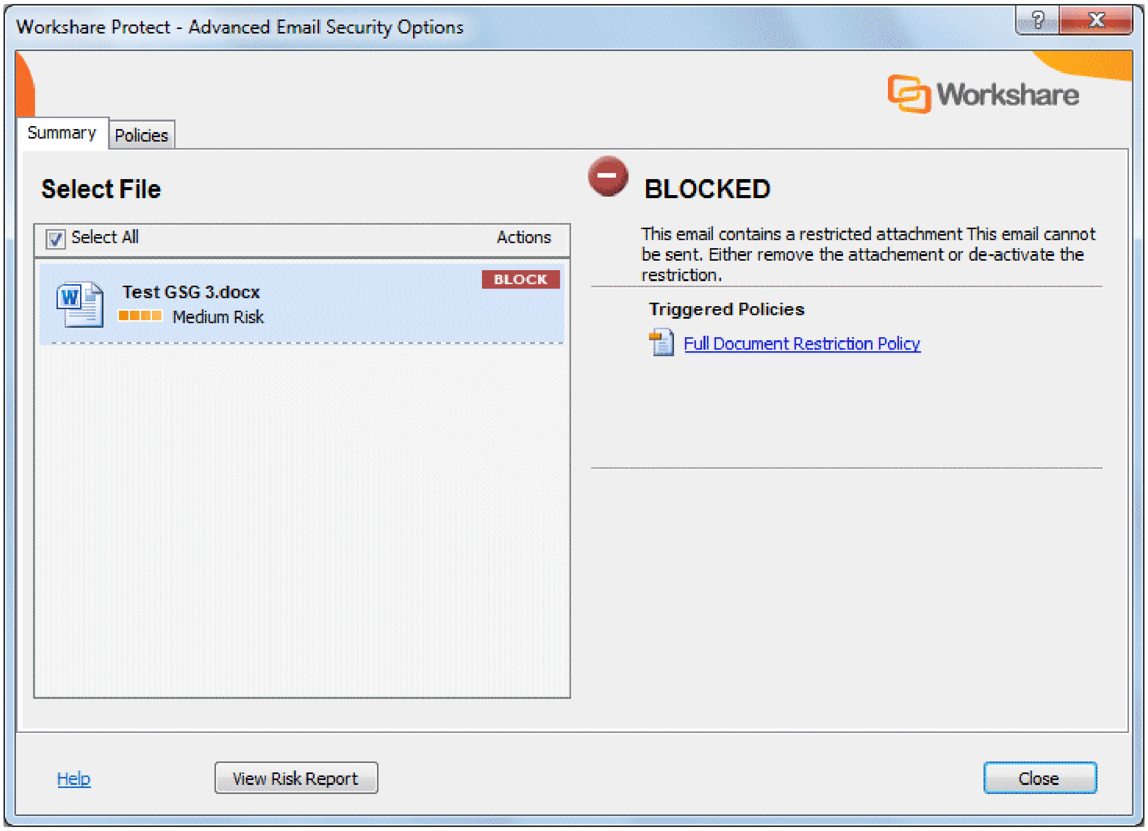
The **Secure File Transfer (SFT)** tab is included in the *Email Security* dialog when a Secure File Transfer profile is selected in the *Protect Profile* dialog. Refer to *Secure File Transfer Profiles*, page 42.

Resolving Blocked Emails

Every time you send an email with an attachment, Workshare Protect checks the attachment to see if it breaches any security policies in the default profile.

Your system administrator can define policies that block any attempt to send emails containing certain pre-defined policy triggers. An attempt to send an email or attachment that contains one of these policy triggers results in the email being blocked. If an email is blocked, the conditions that caused it to be blocked (content, attachment, or recipients) must be removed before the email can be sent.

When you send an email that triggers a **Block** action, Workshare Protect notifies you that your email has been blocked.



BLOCKED

This email contains a restricted attachment This email cannot be sent. Either remove the attachement or de-activate the restriction.

Triggered Policies

Full Document Restriction Policy

To resolve blocked emails:

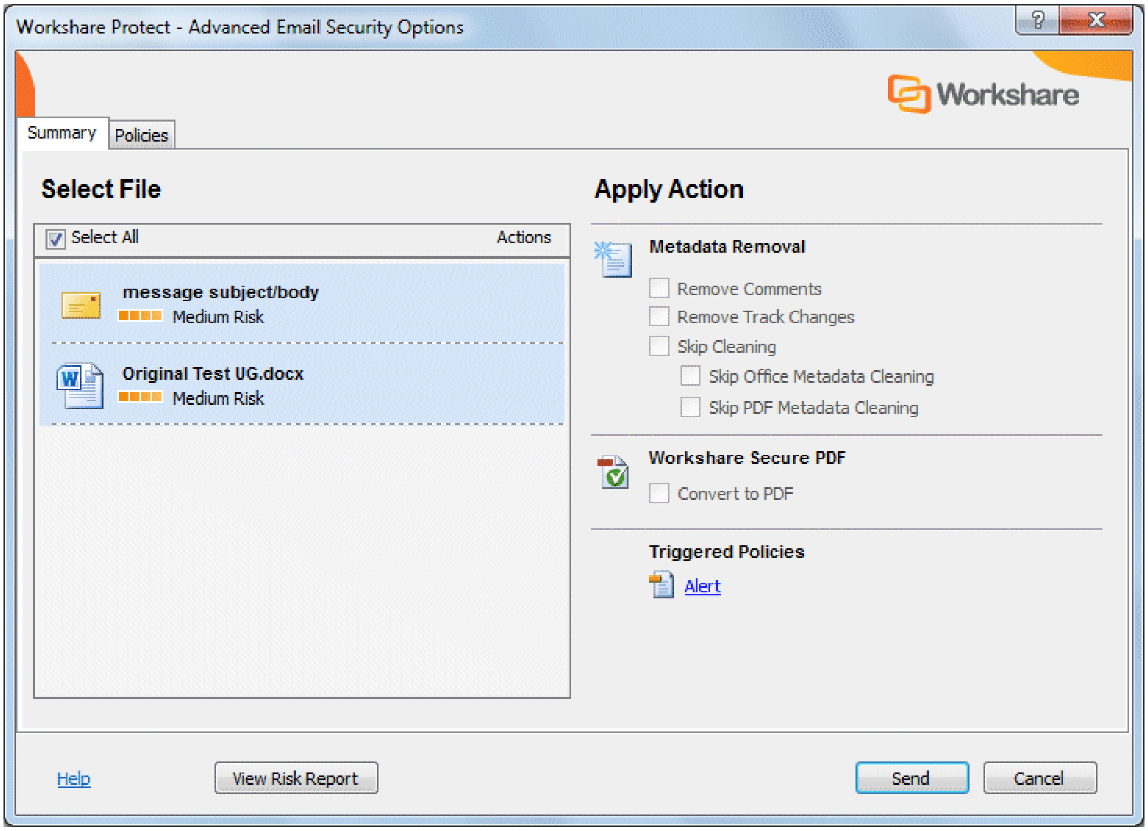
1. Click the name of the policy in the **Triggered Policies** list or select the **Policies** tab to view what content has triggered the email policy.
2. Click the **Close** button to close the *Email Security* dialog.
3. Make the appropriate changes to the email and/or document(s) by removing or modifying the content, attachments or recipients that caused your email to be blocked.
4. If making changes to attachments, re-attach the corrected documents.
5. Click **Send**. If you have made all the relevant changes, you should now be able to send the email successfully.

Reviewing Alerts

Every time you send an email with an attachment, Workshare Protect checks the attachment to see if it breaches any security policies in the default profile.

Your system administrator can define policies that contain certain pre-defined policy triggers that alert you to content risk in emails and documents when they are sent by email. The **Alert** action provides information about content or attachments that might violate policy, but does not require that the content be removed before sending the email.

When you send an email that triggers an **Alert** action, Workshare Protect notifies you that your email and/or attachment(s) contain content risk.



Workshare Protect - Advanced Email Security Options

Summary | Policies

Select File

☑ Select All — Actions

message subject/body — Medium Risk

Original Test UG.docx — Medium Risk

Apply Action

Metadata Removal

□ Remove Comments
□ Remove Track Changes
□ Skip Cleaning
  □ Skip Office Metadata Cleaning
  □ Skip PDF Metadata Cleaning

Workshare Secure PDF

□ Convert to PDF

Triggered Policies

Alert

To find out more about what triggered a policy, click the name of the policy in the **Triggered Policies** list or select the **Policies** tab. The Policies tab is displayed showing the policies triggered on the right side. Click **More**/**Less** to display/hide details of each policy as required. If required, you can make changes to your email or the attached documents to take account of the content risk discovered.

When you are ready to send the email, click **Send**.

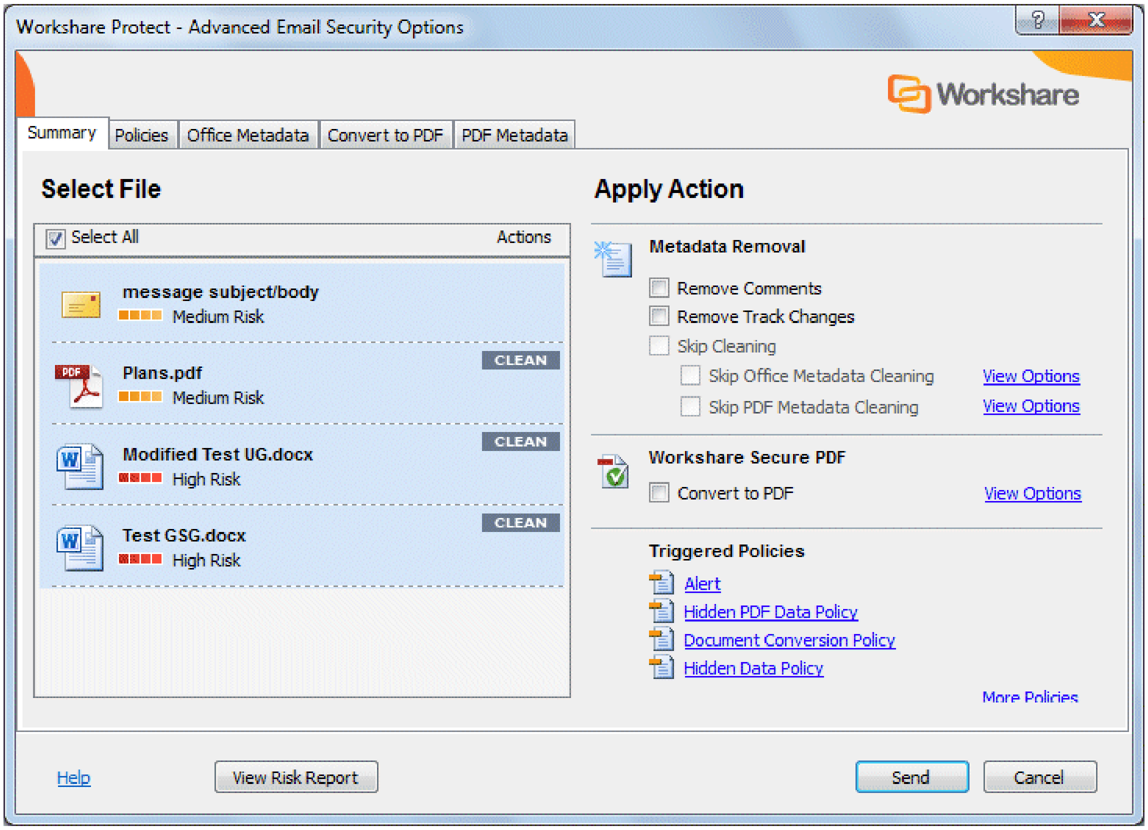
Cleaning Hidden Data from Attachments

Every time you send an email with an attachment, Workshare Protect checks the attachment to see if it breaches any security policies in the default profile.

Your system administrator can define policies that contain certain pre-defined policy triggers that oblige you to clean hidden data from attached documents when they are sent by email. The **Clean**, **Lightspeed Clean** and **PDF Clean** actions remove hidden data, such as track changes, hidden text, comments, markup and more, from attachments.

Lightspeed cleaning is much faster than regular cleaning because it maintains the original structure of the document but redacts hidden data which might contain sensitive information. Thus regular cleaning actually removes the hidden data element from the document whereas Lightspeed cleaning leaves the element but redacts it. With Lightspeed cleaning, formatting track changes which pose no risk are left intact. For a detailed description of what is cleaned using each method of cleaning, refer to Appendix B: Clean and Lightspeed Clean.

When you send an email that triggers a **Clean**, **Lightspeed Clean** or **PDF Clean** action, Workshare Protect notifies you that your email and/or attachment(s) will be cleaned.



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All — Actions

File	Risk	Action
message subject/body	Medium Risk	
Plans.pdf	Medium Risk	CLEAN
Modified Test UG.docx	High Risk	CLEAN
Test GSG.docx	High Risk	CLEAN

Apply Action

Metadata Removal

- □ Remove Comments
- □ Remove Track Changes
- □ Skip Cleaning
  - □ Skip Office Metadata Cleaning — View Options
  - □ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

- □ Convert to PDF — View Options

Triggered Policies

- Alert
- Hidden PDF Data Policy
- Document Conversion Policy
- Hidden Data Policy

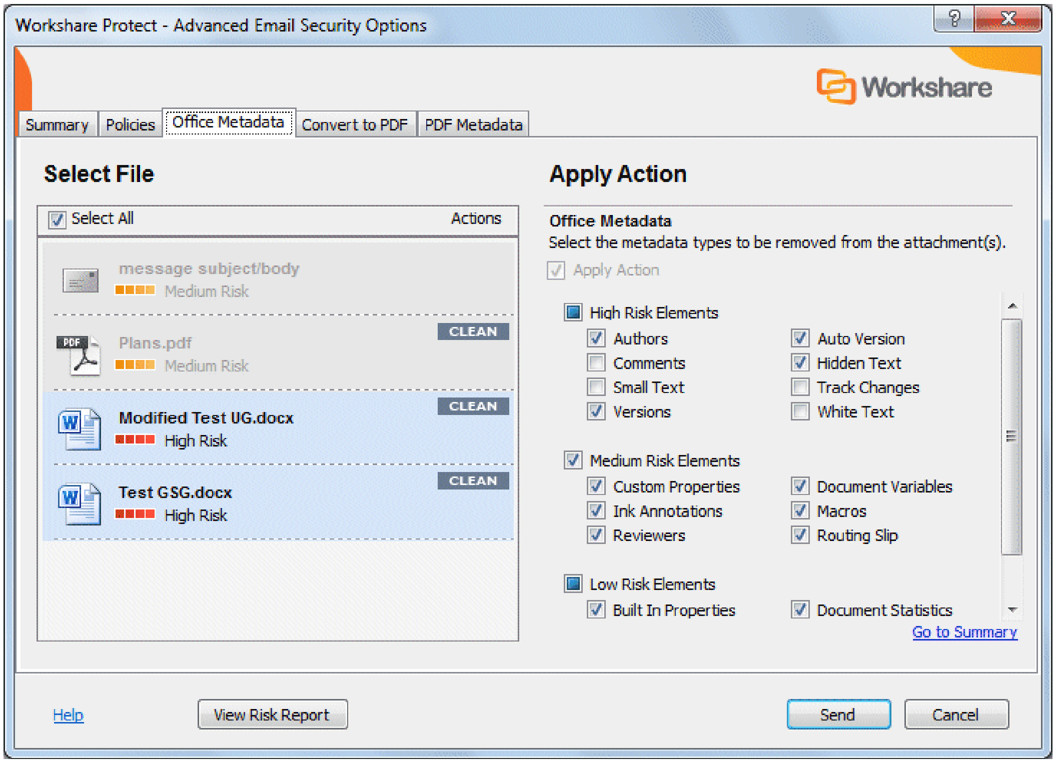
More Policies

> ***Note:** For more information on the types of hidden data contained within Microsoft Office documents, see Overview – Managing Content Risk in Documents.*

If your administrator has enabled you to override the clean hidden data settings and you do not want to clean the attachment(s), you can select the **Skip Cleaning** checkbox (or either of the **Skip Office Metadata Cleaning** or **Skip PDF Metadata Cleaning** checkboxes individually) in the **Apply Action** area.

To clean hidden data:

1. Select the attachment in the **Select File** list to specify individual options for a single attachment or select the **Select All** checkbox to select all attachments. Any settings will then be applied to all attachments.
2. Click **View Options** in the **Metadata Removal** area or select the **Office Metadata** tab. The **Office Metadata** tab displays the different hidden data cleaning options for Microsoft Office attachments.



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All — Actions

- message subject/body — Medium Risk
- Plans.pdf — Medium Risk — CLEAN
- Modified Test UG.docx — High Risk — CLEAN
- Test GSG.docx — High Risk — CLEAN

Apply Action

Office Metadata

Select the metadata types to be removed from the attachment(s).

☑ Apply Action

▣ High Risk Elements

☑ Authors — ☑ Auto Version
☐ Comments — ☑ Hidden Text
☐ Small Text — ☐ Track Changes
☑ Versions — ☐ White Text

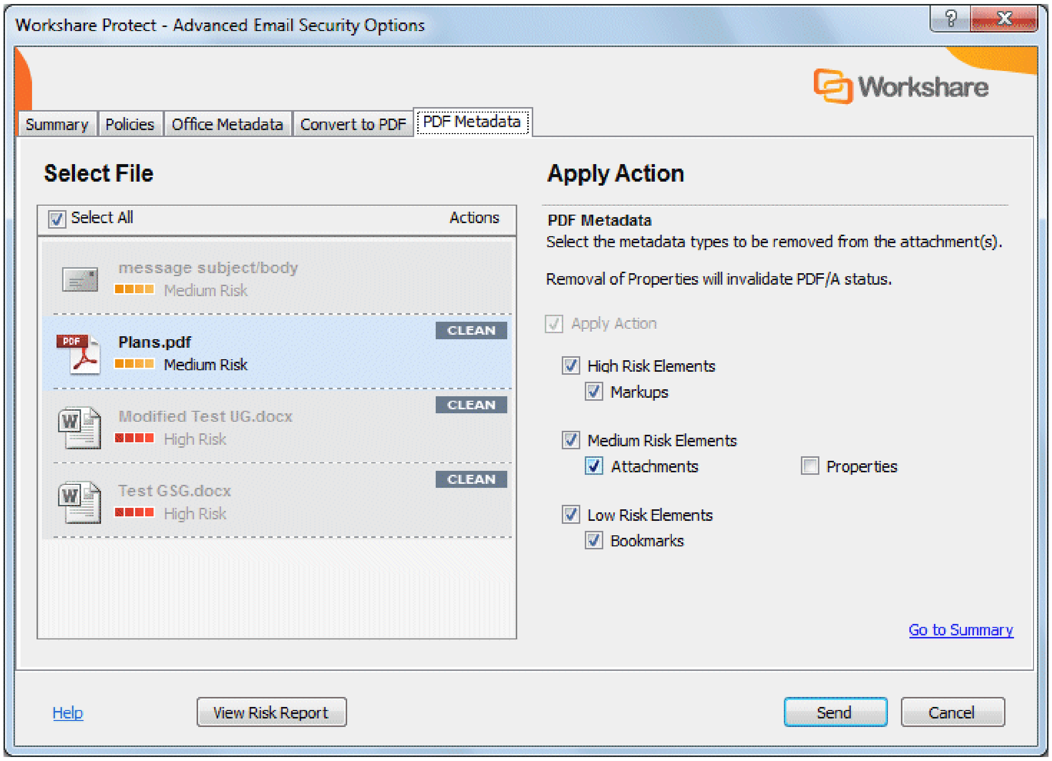
☑ Medium Risk Elements

☑ Custom Properties — ☑ Document Variables
☑ Ink Annotations — ☑ Macros
☑ Reviewers — ☑ Routing Slip

▣ Low Risk Elements

☑ Built In Properties — ☑ Document Statistics

3. Click **View Options** in the **Metadata Removal** area or select the **PDF Metadata** tab to display the different hidden data cleaning options for PDF attachments.



Select File

☑ Select All — Actions

message subject/body — Medium Risk

Plans.pdf — Medium Risk — CLEAN

Modified Test UG.docx — High Risk — CLEAN

Test GSG.docx — High Risk — CLEAN

Apply Action

PDF Metadata
Select the metadata types to be removed from the attachment(s).

Removal of Properties will invalidate PDF/A status.

☑ Apply Action

☑ High Risk Elements
☑ Markups

☑ Medium Risk Elements
☑ Attachments ☐ Properties

☑ Low Risk Elements
☑ Bookmarks

Note: *The availability of these options is dependent on whether your administrator has enabled you to override the cleaning options in the policy settings. Refer to your system administrator if you need to override these settings and they are disabled.*

4. Select the hidden data that you want to remove by selecting or deselecting the relevant checkboxes.

5. Repeat for additional attachments if required.

6. Click **Send** to send the email.

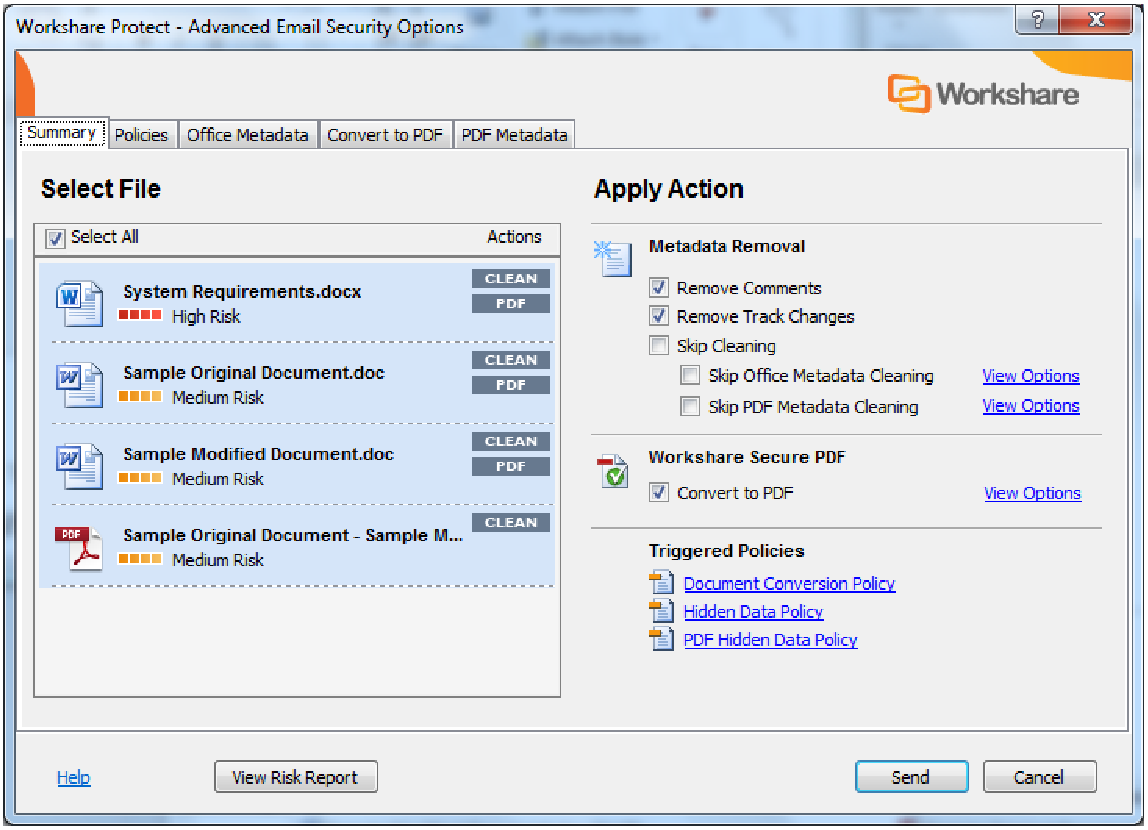
Workshare Protect cleans the hidden data from the attached document(s) according to your settings before sending the email.

Converting Attachments to PDF

Every time you send an email with an attachment, Workshare Protect checks the attachment to see if it breaches any security policies in the default profile.

Your system administrator can define policies that contain certain pre-defined policy triggers that force you to convert documents to PDF when they are sent by email. This prevents the document from being edited, ensuring that its formatting remains intact. Additional security features enable you to prevent recipients from printing, editing, copying from or adding comments to the PDF attachment.

When you send an email that triggers a **PDF** action, Workshare Protect notifies you that your attachment(s) will be converted to PDF.



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All — Actions

File	Risk	Actions
System Requirements.docx	High Risk	CLEAN PDF
Sample Original Document.doc	Medium Risk	CLEAN PDF
Sample Modified Document.doc	Medium Risk	CLEAN PDF
Sample Original Document - Sample M...	Medium Risk	CLEAN

Apply Action

Metadata Removal

- ☑ Remove Comments
- ☑ Remove Track Changes
- □ Skip Cleaning
  - □ Skip Office Metadata Cleaning — View Options
  - □ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

- ☑ Convert to PDF — View Options

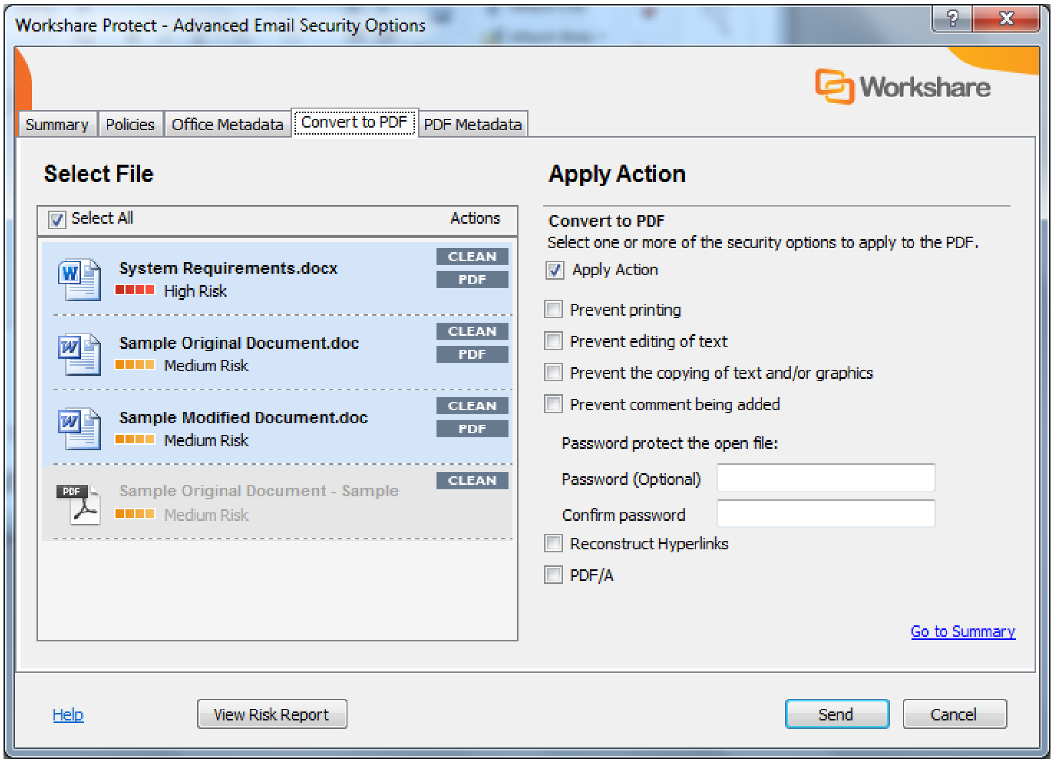
Triggered Policies

- Document Conversion Policy
- Hidden Data Policy
- PDF Hidden Data Policy

If your administrator has enabled you to override the PDF settings and you do not want to PDF the attachment(s), you can deselect the **Convert to PDF** checkbox in the **Apply Action** area.

To convert attachments to PDF:

1. Select the attachment in the **Select File** list and click **View Options** in the **Workshare Secure PDF** area or select the **Convert to PDF** tab. The **Convert to PDF** tab displays the different PDF security settings available.



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All — Actions

- System Requirements.docx — 🟥🟥🟥🟥 High Risk — CLEAN, PDF
- Sample Original Document.doc — 🟧🟧🟧🟧 Medium Risk — CLEAN, PDF
- Sample Modified Document.doc — 🟧🟧🟧🟧 Medium Risk — CLEAN, PDF
- Sample Original Document - Sample — 🟧🟧🟧🟧 Medium Risk — CLEAN

Apply Action

Convert to PDF

Select one or more of the security options to apply to the PDF.

☑ Apply Action

□ Prevent printing

□ Prevent editing of text

□ Prevent the copying of text and/or graphics

□ Prevent comment being added

Password protect the open file:

Password (Optional)

Confirm password

□ Reconstruct Hyperlinks

□ PDF/A

> ***Note:*** *You can specify individual PDF settings for each attachment or select the* ***Select All*** *button.*

2. Select one or more of the following security options:
   - **Prevent printing** to prevent recipients from printing the PDF document.
   - **Prevent editing of text** to prevent recipients with Adobe Distiller from editing the PDF document.
   - **Prevent the copying of text and/or graphics** to prevent recipients from copying graphics or text directly from the PDF document.
   - **Prevent comments being added** to prevent recipients with Adobe Distiller from adding comments to the PDF document.

> ***Note:*** *Highlighting text and adding a strikethrough in a PDF is not considered editing the text. If you want to prevent users doing this, select* ***Prevent comments being added*** *as well as* ***Prevent editing of text****.*

3. If required, set a password for access to the PDF by entering the password twice in the relevant fields.

4. If required, select the **Reconstruct Hyperlinks** checkbox to preserve standard URL and bookmark hyperlinks.

> ***Note:*** *Selecting the* ***Reconstruct Hyperlinks*** *option can increase the time it takes to create a PDF document. Hyperlinks that are preserved using this option may not correspond exactly to the location in the original document.*

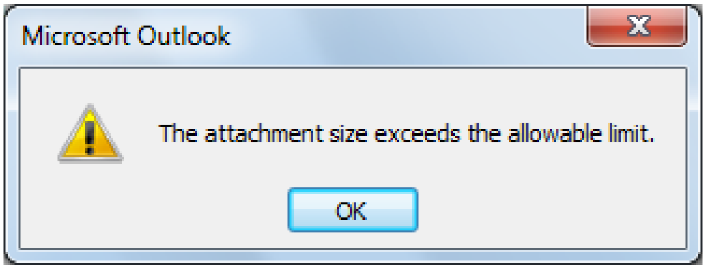
5. Select the PDF/A checkbox to convert the attachment to PDF/A.
6. Repeat steps 2 to 5 for additional attachments if required.
7. Click **Send** to send the email.

Workshare Protect converts the attachments to PDF or PDF/A and applies your settings before sending the email.

Sending Large Files

When your administrator has set a limit on the size of files you can email (to avoid large files blocking Exchange), you can use Secure File Transfer functionality to send a link to the large files.

When you try and add a file with a size over the specified limit, Microsoft Outlook displays a message such as:



Microsoft Outlook

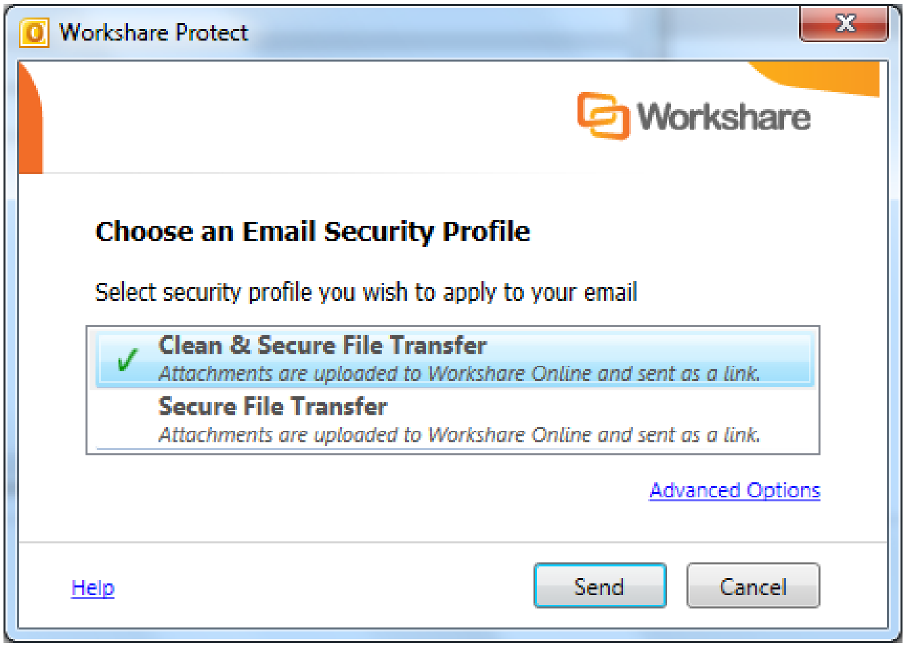
The attachment size exceeds the allowable limit.

In this case, you can use the **Add Large Attachment** button to access the Secure File Transfer functionality.

To send large files:

1. Open a new email message window.
2. Click **Add Large Attachment**.
3. Browse to the large file you want to attach and click **Open**. The attachment displayed in the message appears small because it is only a pointer to the large file.

4. Add the recipient and message details and click **Send**. The Protect Profile dialog is displayed with only the Secure File Transfer profiles available.



Choose an Email Security Profile

Select security profile you wish to apply to your email

✓ Clean & Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

Secure File Transfer
Attachments are uploaded to Workshare Online and sent as a link.

5. Select the required Secure File Transfer profile and click **Send**.

The attached large file is uploaded to a folder in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time. This folder appears in your Sent Items folder in My Files and Folders in Workshare. The recipient receives an email notifying them that file has been uploaded to Workshare and providing a link to the file.

***Note**: The **Add Large Attachment** button does not work with Interactive Protect; it is disabled.*

Chapter 5. Controlling Documents

This chapter describes how to control your documents by setting restrictions on whether or not they can be emailed. It includes the following sections:

- **Document Classification**, below, introduces the classification levels available in Workshare Protect.
- **Setting Classification Levels**, page 63, describes how to classify a document.
- **Emailing Classified Documents**, page 65, describes the effect a classification level has on a document when it is emailed.

Document Classification

Workshare Protect enables you to restrict access to sensitive business documents by classifying documents. This classification controls the distribution of documents by email - it can prevent documents from being emailed either to any user, or to external users or it can alert users to the potentially sensitive nature of the document they are attempting to email.

Workshare Protect provides the following default classification levels:

- **For Internal Use Only**: The document is restricted and can only be distributed internally within your organization. Use this status if you are collaborating on a document with colleagues, but the document is not yet ready for client review.
- **Confidential**: The document contains information of a confidential nature and when emailed either externally or internally, you are alerted to the fact that the document contains confidential information. You can still send the document to any recipient.

> ***Note**: When working with the Workshare Protect Profile dialog, you do not receive an alert and you can send the document to any recipient unless you configure a policy to implement other behavior.*

- **Highly Confidential**: The document contains information of a highly confidential nature and when emailed whether externally or internally, it will be blocked.

> ***Note**: When working with the Workshare Protect Profile dialog, the email is not blocked and you can send the document to any recipient unless you configure a policy to implement other behavior.*

- **External Restriction**: The document is restricted and can only be distributed internally within your organization. Use this status if you are collaborating on a document with colleagues, but the document is not yet ready for client review.
- **Full Restriction**: The document is restricted and cannot be distributed via email. Use this status if you are working on a document yourself and do not want it distributed.

These classification levels can be password-protected. This ensures that only users who know the password can remove or alter a classification status from documents.

> ***Note:*** *The names and descriptions of the classification levels are defined in the ClassificationList.xml file located in the Workshare Protect installation folder. The names of the classification levels can be amended or classification levels can be deleted or additional classification levels can be added by editing this file.*

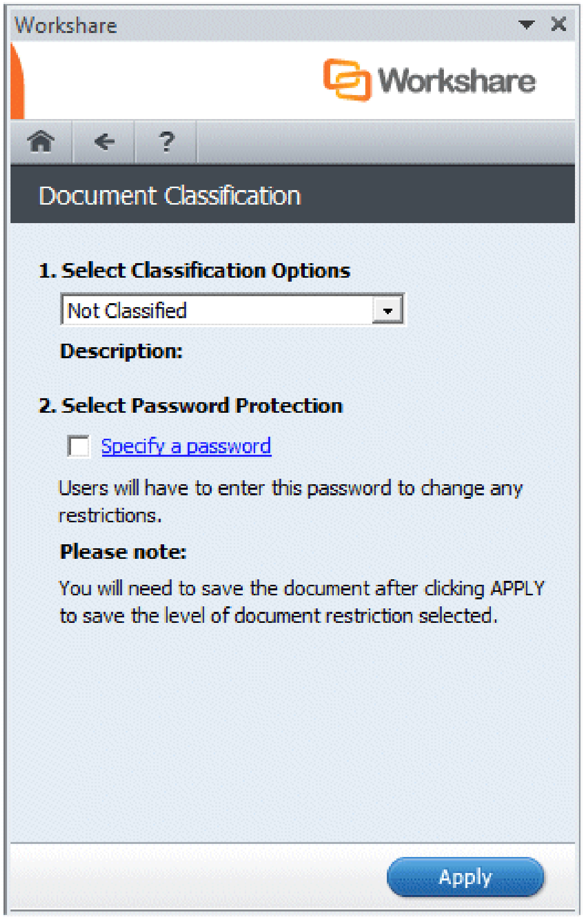
In previous versions of Workshare Protect, three restrictions were available: **No Restriction** (as if no classification level is set), **External Restriction**, and **Full Restriction**. If you would prefer to work with only these three classification levels, you can edit the ClassificationList.xml file accordingly.

Setting Classification Levels

Documents are classified from the Document Classification page of the Workshare Panel. If required, you can password-protect a classification level so that only users who know the password can remove or change a classification level for a document.

To set a classification level:

1. With your document open in Microsoft Word, Excel or PowerPoint, click **Classify** (**Protect** group) in the *Workshare* tab or click **Classify** in the Home page of the Workshare Panel. The Document Classification page is displayed.



Document Classification

1. Select Classification Options

Not Classified

Description:

2. Select Password Protection

□ Specify a password

Users will have to enter this password to change any restrictions.

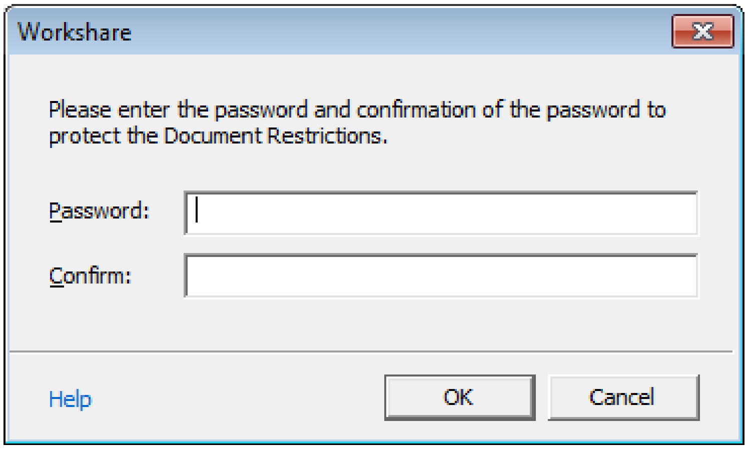
Please note:

You will need to save the document after clicking APPLY to save the level of document restriction selected.

2. Select the classification level you require for the open document from the following:
   - **For Internal Use Only**: The document is restricted and can only be distributed internally within your organization. Use this status if you are collaborating on a document with colleagues, but the document is not yet ready for client review.
   - **Confidential**: The document contains information of a confidential nature and when emailed either externally or internally, you are alerted to the fact that the document contains confidential information. You can still send the document to any recipient.
   - **Highly Confidential**: The document contains information of a highly confidential nature and when emailed whether externally or internally, it will be blocked.
   - **External Restriction**: The document is restricted and can only be distributed internally within your organization. Use this status if you are collaborating on a document with colleagues, but the document is not yet ready for client review.
   - **Full Restriction**: The document is restricted and cannot be distributed via email. Use this status if you are working on a document yourself and do not want it distributed.

3. If you want to password-protect the classification level, select the **Specify a password** checkbox in the **Select Password Protection** area. This means that only those who know the password can change the classification level of the document.

4. Click **Apply**. If you selected the **Specify a password** checkbox, you are prompted for a password.



Workshare

Please enter the password and confirmation of the password to protect the Document Restrictions.

Password:

Confirm:

Tip! *If you click the words* ***Specify a password*** *in the Document Classification page, the above dialog is displayed immediately before clicking* ***Apply****.*

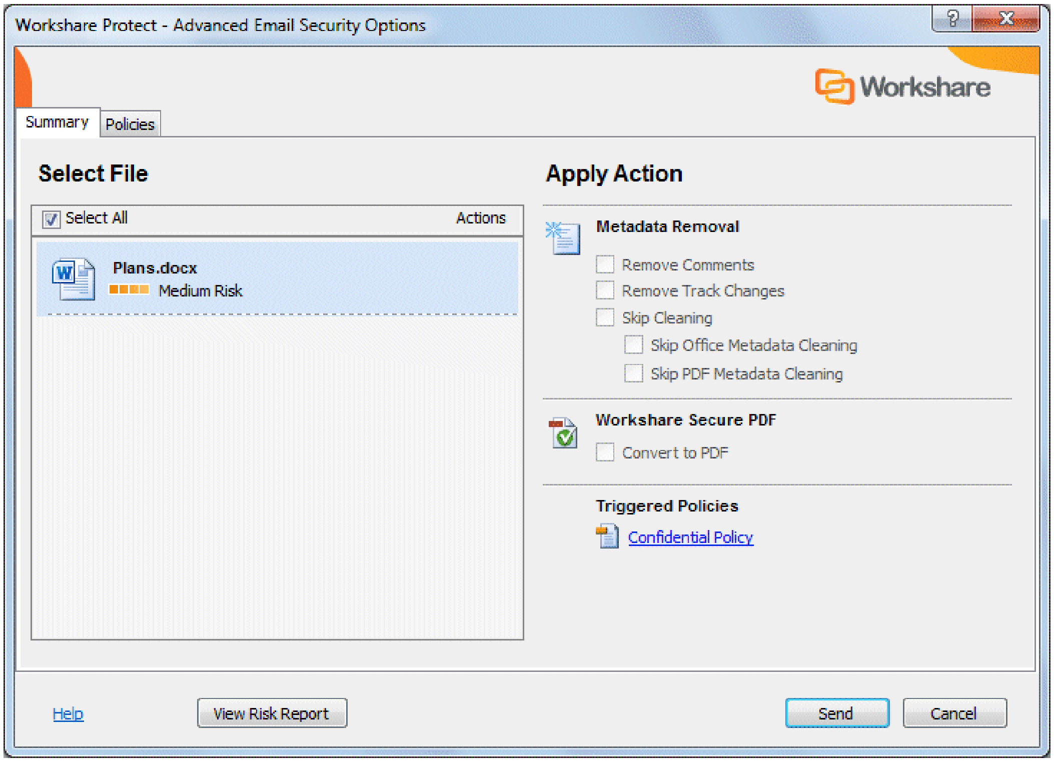
5. Enter the password twice to set and confirm the password and click **OK**.

6. Save the document. The open document is now restricted according to the selected classification level.

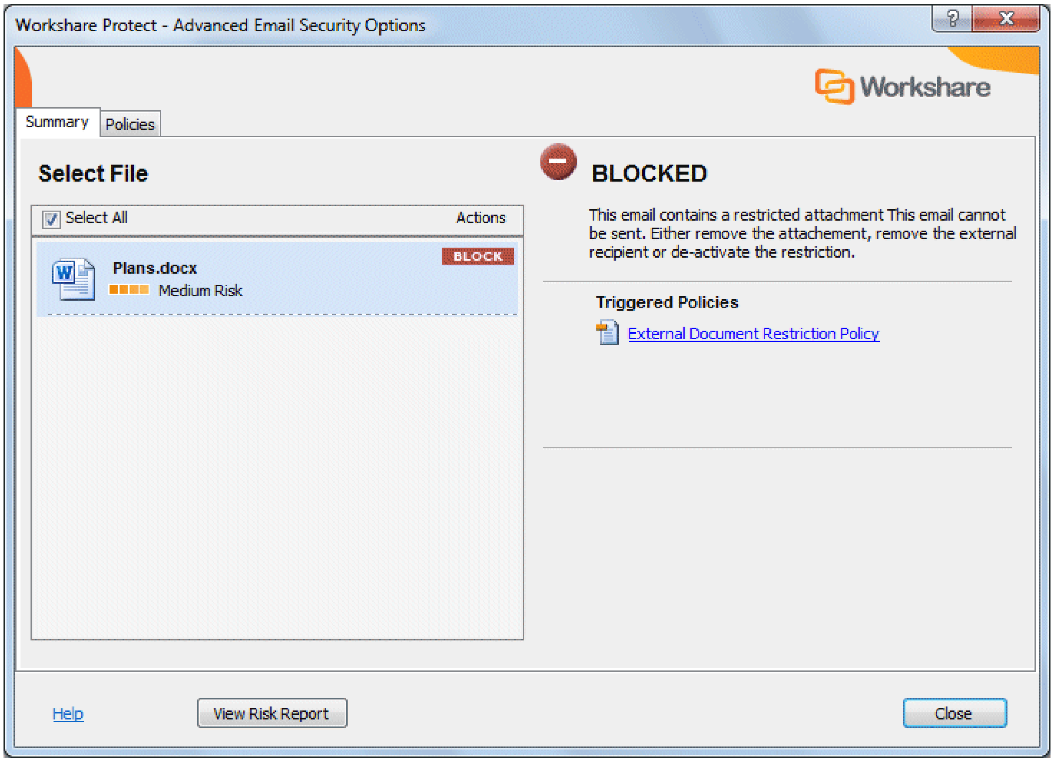
Emailing Classified Documents

When a document is emailed, the classification level is checked and the document is handled according to its classification level:

- If the document has a **Not Classified** classification, it is emailed without any warning.
- If the document has a **Confidential** classification, you will receive an alert when trying to email it. You can still send the email with the attached document by clicking **Send**.



- If the document has a **For Internal Use** or **External Restriction** classification, it can be freely emailed to internal recipients. However, if you try to email it to an external recipient, the following dialog is displayed:



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All | Actions

Plans.docx — Medium Risk — BLOCK

BLOCKED

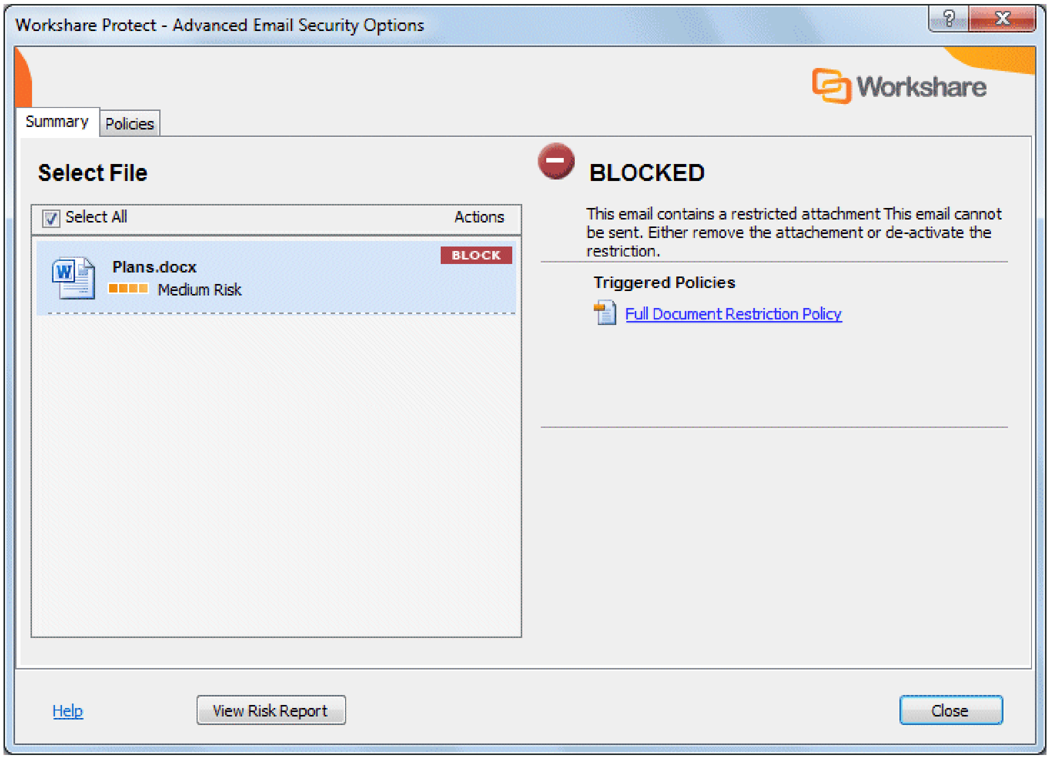
This email contains a restricted attachment This email cannot be sent. Either remove the attachement, remove the external recipient or de-activate the restriction.

Triggered Policies

External Document Restriction Policy

The email cannot be sent. Click **Close** to cancel the email. If you were sending the email to internal and external recipients, you should remove the external recipients and resend to internal recipients only.

- If the document has a **Highly Confidential** or **Full Restriction** classification, it cannot be emailed at all. If you try to email it, the following dialog is displayed.



This email contains a restricted attachment This email cannot be sent. Either remove the attachement or de-activate the restriction.

The email cannot be sent. Click **Close** to cancel the email.

Chapter 6. Converting to PDF

This chapter describes how to convert your documents to PDF using Workshare Protect. It includes the following sections:

- **Overview**, below, introduces the PDF conversion functionality available in Workshare Protect.
- **Creating PDFs**, page 69, describes how to convert a document to PDF.
- **PDF From Anywhere**, page 73, describes how to create a PDF from any application.

Overview – Converting to PDF

Workshare Protect creates the most secure PDF files available from any application. You can quickly and easily convert open and closed Microsoft Office documents into PDF or PDF/A. You can also enforce PDF creation on email attachments leaving your organization. When sending documents for review, you can convert to PDF or PDF/A any comparison documents or additional documents included. In all these circumstances, before converting to PDF, Workshare Protect offers you the opportunity to remove hidden data from the document and set PDF security options. Workshare Protect also provides “PDF Anywhere”. This is the ability to convert a document to PDF from any application.

Converting Documents to PDF

Workshare Protect enables you to quickly and easily convert Microsoft Word, Excel and PowerPoint documents into PDF (Portable Document Format) or PDF/A. This functionality is available from within an open document or when the document is closed. Before Workshare Protect converts the document, you can select to remove sensitive hidden data from the document. Refer to Creating PDFs.

PDF and Emails

Workshare Protect provides organizations with the ability to enforce PDF creation on documents leaving the organization through policy rules. Your system administrator can create policies that contain certain pre-defined policy triggers that force you to convert documents to PDF when they are sent by email. Refer to Converting Attachments to PDF.

Additionally, Workshare Protect enables you to quickly and easily convert open Microsoft Word, Excel and PowerPoint documents into PDF or PDF/A and send them by email. Before Workshare Protect converts the document, you can select to remove sensitive hidden data from the document. Refer to Creating PDFs.

PDF Anywhere

Workshare Protect enables you to create and combine PDF files from any application, for example, an email application, a browser or Notepad. You can convert to a new PDF file or you append to an existing PDF file. Refer to PDF From Anywhere.

Creating PDFs

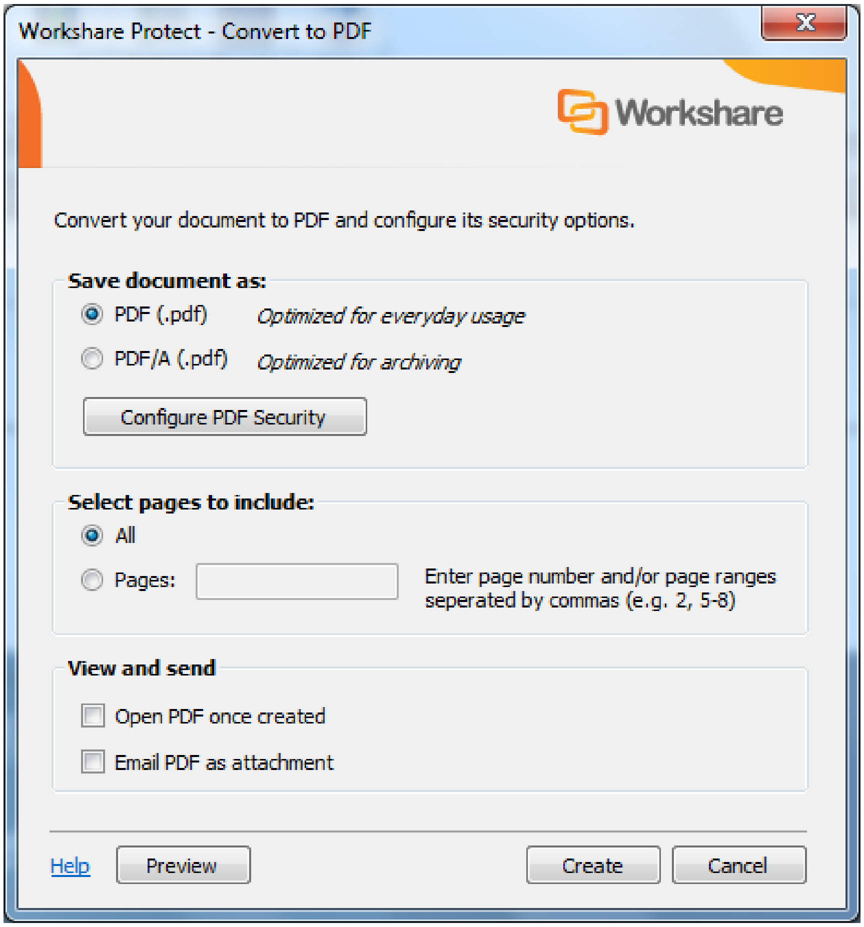
At any time when working on a document in Microsoft Word, Excel or PowerPoint, you can convert the document into PDF or PDF/A. This is useful if you want to maintain a file in its current format, as PDF documents cannot be edited as easily as Microsoft Word, Excel and PowerPoint documents. This functionality is available from within an open document or when the document is closed.

Open Documents

Workshare Protect automatically saves a document before converting to PDF or PDF/A. Documents can be stored locally, in SharePoint or in your DMS.

To convert an open document to PDF or PDF/A:

1. With your document open in Microsoft Word, Excel or PowerPoint, click **Convert to PDF** (**Protect** group) in the Workshare tab or click **Convert to PDF** in the Home page of the Workshare Panel. The *Convert to PDF* dialog is displayed.



Workshare Protect - Convert to PDF

Convert your document to PDF and configure its security options.

Save document as:

● PDF (.pdf) *Optimized for everyday usage*

○ PDF/A (.pdf) *Optimized for archiving*

Configure PDF Security

Select pages to include:

● All

○ Pages: Enter page number and/or page ranges seperated by commas (e.g. 2, 5-8)

View and send

□ Open PDF once created

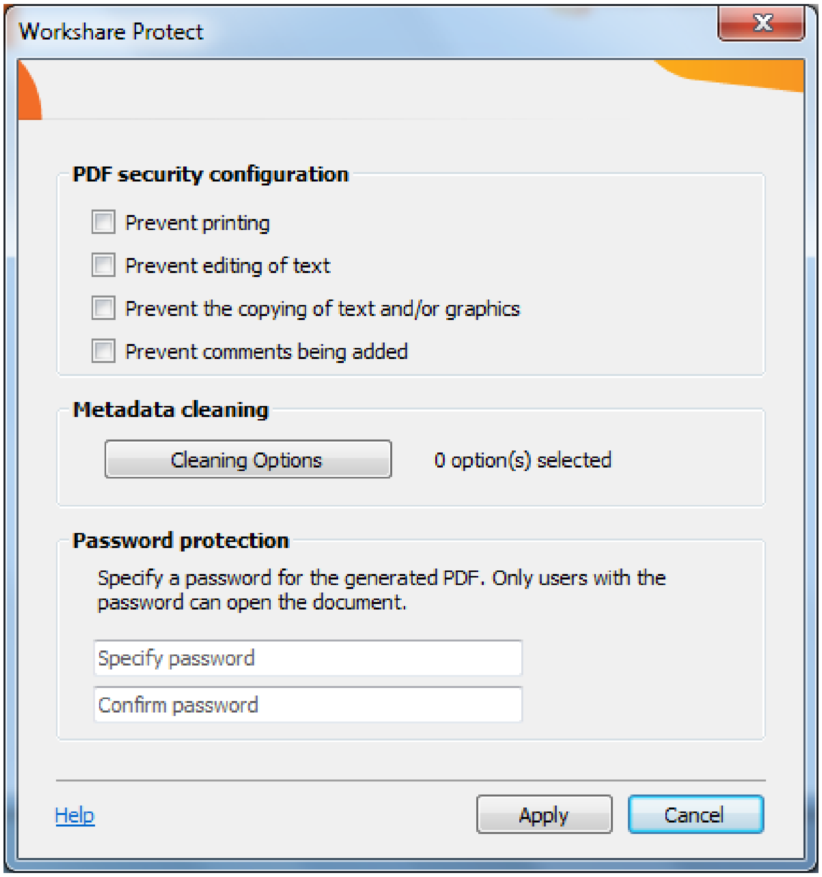
□ Email PDF as attachment

Help | Preview | Create | Cancel

> ***Note:*** *If working with a DMS, the dialog looks slightly different to the one above and you can select whether to save the PDF as a new document or related document in your DMS or as a local file.*

2. Select whether to convert to PDF or PDF/A.

3. Click **Configure PDF Security** to set PDF security options and remove metadata.



Workshare Protect

PDF security configuration

□ Prevent printing

□ Prevent editing of text

□ Prevent the copying of text and/or graphics

□ Prevent comments being added

Metadata cleaning

0 option(s) selected

Password protection

Specify a password for the generated PDF. Only users with the password can open the document.

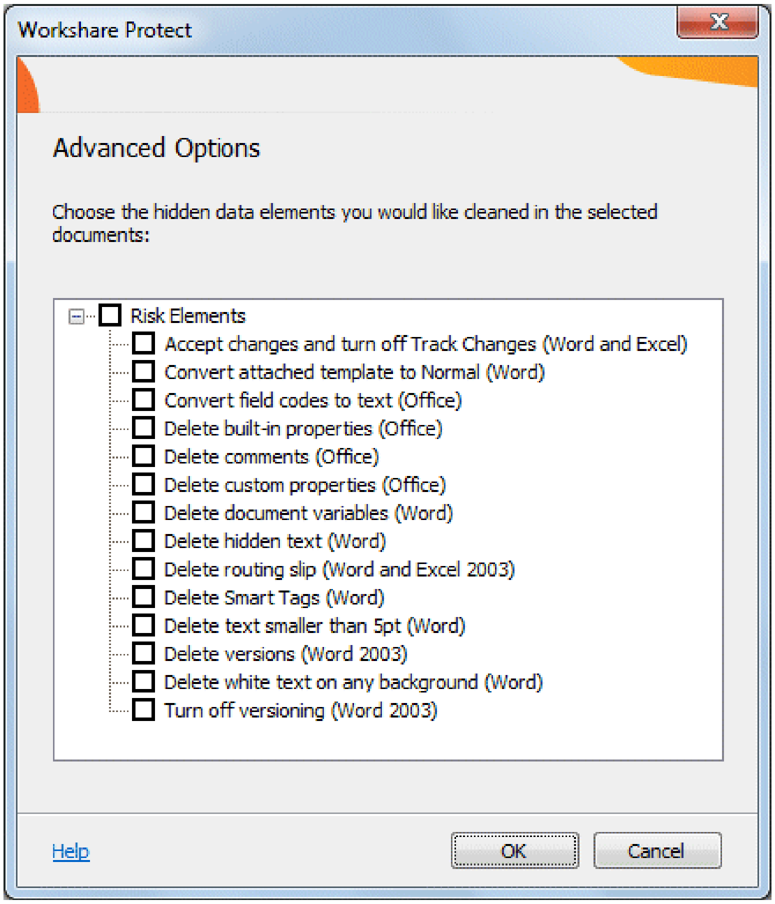
Specify password

Confirm password

4. Select one or more of the following security options:
   - **Prevent printing:** Prevents recipients from printing the PDF document.
   - **Prevent editing of text:** Prevents recipients with Adobe Distiller from editing the PDF document.
   - **Prevent the copying of text and/or graphics:** Prevents recipients from copying graphics or text directly from the PDF document.
   - **Prevent comments being added:** Prevents recipients with Adobe Distiller from adding comments to the PDF document.

> ***Note:*** *These options are disabled and cannot be selected if you selected PDF/A in step 2.*

5. To specify what hidden data to remove before converting it to PDF, click **Cleaning Options**.



Advanced Options

Choose the hidden data elements you would like cleaned in the selected documents:

- □ Risk Elements
  - □ Accept changes and turn off Track Changes (Word and Excel)
  - □ Convert attached template to Normal (Word)
  - □ Convert field codes to text (Office)
  - □ Delete built-in properties (Office)
  - □ Delete comments (Office)
  - □ Delete custom properties (Office)
  - □ Delete document variables (Word)
  - □ Delete hidden text (Word)
  - □ Delete routing slip (Word and Excel 2003)
  - □ Delete Smart Tags (Word)
  - □ Delete text smaller than 5pt (Word)
  - □ Delete versions (Word 2003)
  - □ Delete white text on any background (Word)
  - □ Turn off versioning (Word 2003)

6. Select hidden data elements as required. For a full description of all the hidden data elements, refer to Cleaning Hidden Data for further information.

7. Click **OK**.

8. If required, set a password to protect the PDF by entering the password twice in the **Password protection** area. When a password is specified, the recipient can only open the PDF after entering this password.

> ***Note:*** *If you selected PDF/A in step 2, you cannot set a password and the* ***Password protection*** *area is disabled.*

9. Click **Apply**.

10. In the *Convert to PDF* dialog, if you want to create a PDF of part of the document only, select the **Pages** radio button and specify a page range.

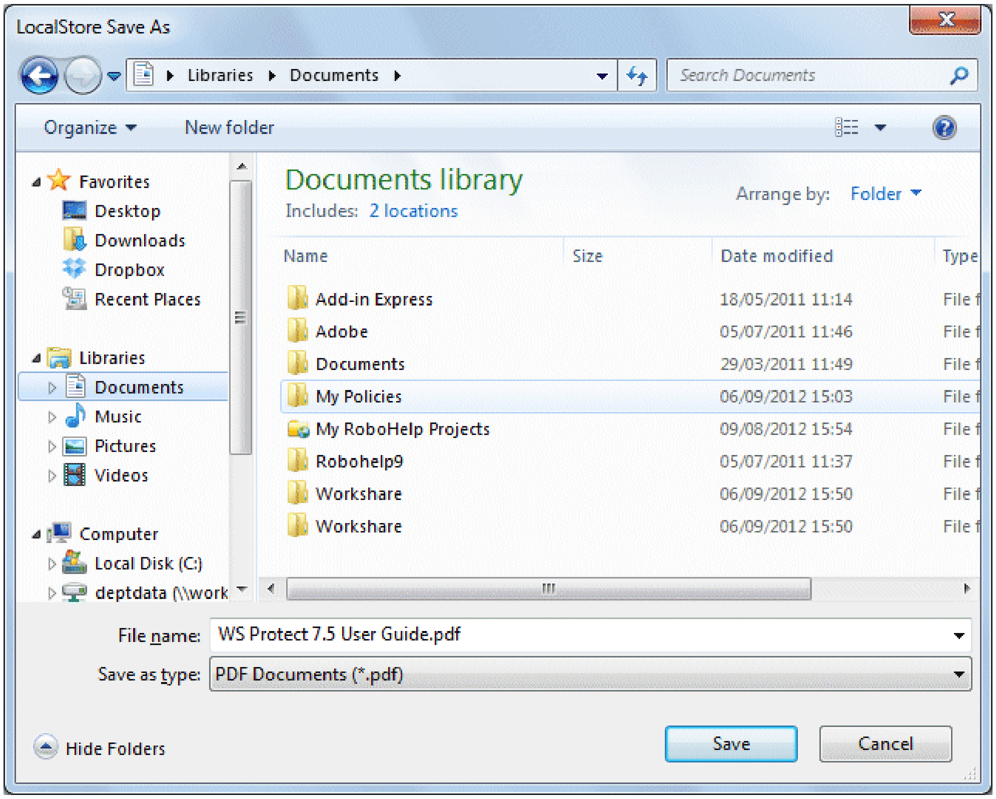
> ***Note:*** *You can also PDF individual pages by specifying the pages (separated by commas) in the* ***Pages*** *field.*

11. Select the **Open PDF once created** checkbox if you want the PDF to be opened once it has been created.

12. Select the **Email PDF as attachment** checkbox if you want the PDF to be attached to an email once it has been created.

13. If required, click **Preview** to view the document as a PDF.

14. Click **Create**. The *Save As* dialog is displayed:



Name	Size	Date modified	Type
Add-in Express		18/05/2011 11:14	File f
Adobe		05/07/2011 11:46	File f
Documents		29/03/2011 11:49	File f
My Policies		06/09/2012 15:03	File f
My RoboHelp Projects		09/08/2012 15:54	File f
Robohelp9		05/07/2011 11:37	File f
Workshare		06/09/2012 15:50	File f
Workshare		06/09/2012 15:50	File f

File name: WS Protect 7.5 User Guide.pdf

Save as type: PDF Documents (*.pdf)

15. Specify the name and location for the PDF file and click **Save**. The document is converted to PDF or PDF/A. If you selected **Open PDF once created**, the new PDF is opened. If you selected **Email PDF as attachment**, an email message window is displayed with the PDF as an attachment.

Closed Documents

Workshare Protect can convert closed Microsoft Word, Excel or PowerPoint documents to PDF or PDF/A.

To convert a closed document to PDF or PDF/A:

- Right-click the closed Microsoft Word, Excel or PowerPoint file on your desktop or DMS and select **Convert to PDF with Workshare** from the menu. The *Convert to PDF* dialog is displayed.

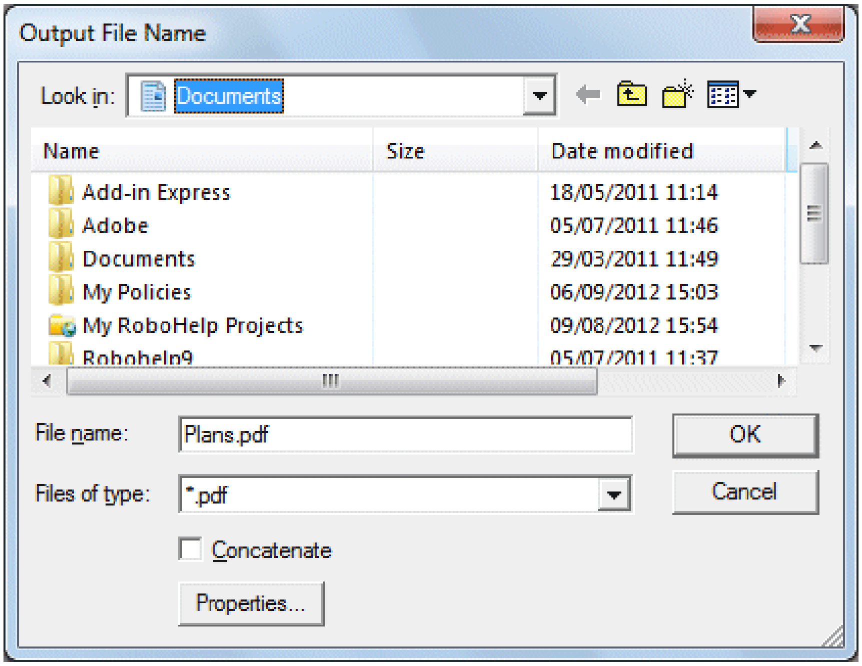
Continue as described in steps 2 to 15 of the Open Documents section.

PDF From Anywhere

Workshare Protect can convert any document or file to PDF, for example, a page in Internet Explorer, an email message or a text file in Notepad. You can create a new PDF from the file or add to an existing PDF.

To convert to PDF from anywhere:

1. Click **Print** in the application.
2. Select **Workshare PDF Publisher** as the printer.
3. Specify other settings as required and click **Print**. The *Output File Name* dialog is displayed.



Output File Name

Look in: Documents

Name	Size	Date modified
Add-in Express		18/05/2011 11:14
Adobe		05/07/2011 11:46
Documents		29/03/2011 11:49
My Policies		06/09/2012 15:03
My RoboHelp Projects		09/08/2012 15:54
Robohelp9		05/07/2011 11:37

File name: Plans.pdf

Files of type: *.pdf

□ Concatenate

4. Specify a name for the PDF in the **File name** field or, if you want to add to an existing PDF, select the **Concatenate** checkbox and browse to and select the existing PDF.
5. Click **OK**. The open document is converted to PDF and saved as specified or added to an existing PDF.

Chapter 7. Configuring Workshare

This chapter describes the Workshare Configuration Manager. It includes the following sections:

- **Introducing the Workshare Configuration Manager**, below, introduces the Workshare configuration utility.
- **Accessing the Workshare Configuration Manager**, below, describes how to access the Workshare Configuration Manager.
- **Setting Parameters**, page 76, describes how to set values for parameters in the Workshare Configuration Manager.

Introducing the Workshare Configuration Manager

The Workshare Configuration Manager is a configuration utility that enables you to configure Workshare and the way it behaves as well as modify the configuration of the Client Default profile (via the parameters in the **Protection** category).

> ***Note**: A profile is a collection of policies. A policy is a set of parameters applied by Workshare Protect when determining content risk.*

Administrator Mode and User Mode

The Workshare Configuration Manager has two modes as follows:

- **Administrator Mode**: This mode is for administrators to make changes to the default settings on the local machine. Settings made are saved in HKEY_LOCAL_MACHINE in the Registry. As a user you will only have access to Administrator mode if you have Administrator rights.
- **User Mode**: This mode is for users to make changes to the Workshare configuration to suit their own personal preferences on the local machine. Other users could log in and they would not have the same configuration settings. Settings made are personal to the user and saved in HKEY_CURRENT_USER in the Registry.

> ***Note:** Your system administrator may have restricted the rights of users to modify configuration parameters by locking individual parameters so that users cannot override the setting. If you have restricted access rights and have special requirements for configuration, please speak to your system administrator.*

Accessing the Workshare Configuration Manager

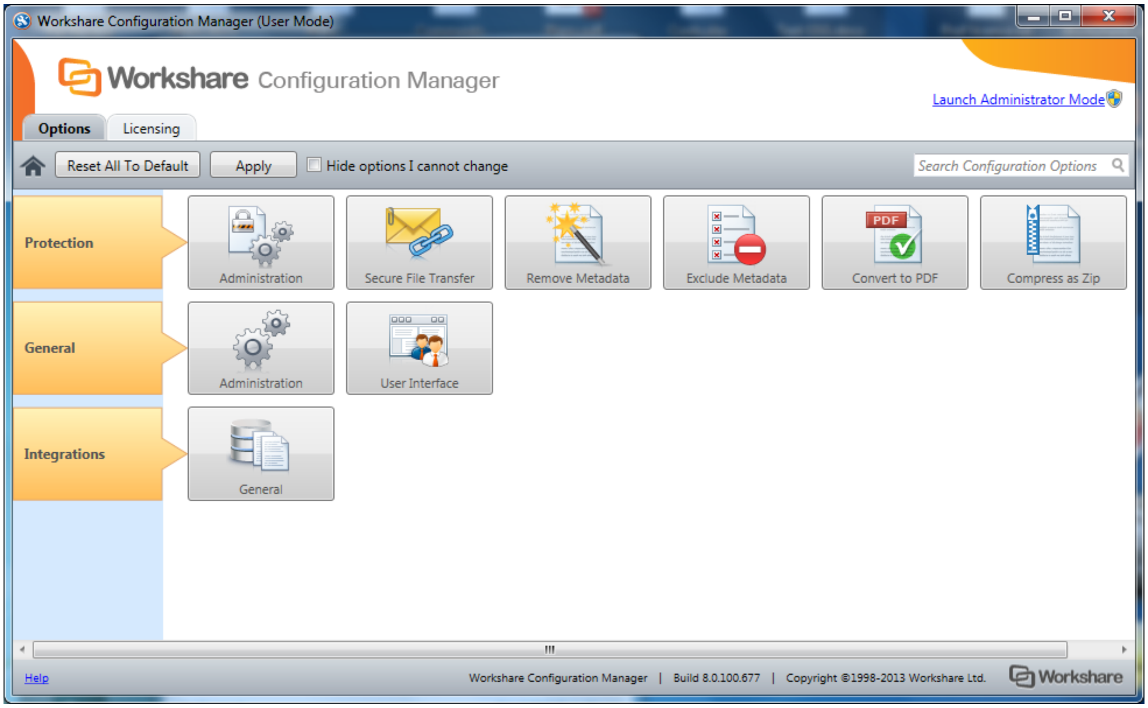
The Workshare Configuration Manager can be accessed from within Microsoft Word or from the Start menu.

To access the Workshare Configuration Manager from Microsoft Word:

- In Microsoft Word, click **Options** in the *Workshare* tab, **Options** group. The Workshare Configuration Manager opens in User Mode.

To access the Workshare Configuration Manager from the Start menu:

- From the Start menu, select **All Programs** > **Workshare** > **Workshare Configuration**. The Workshare Configuration Manager opens in User Mode.

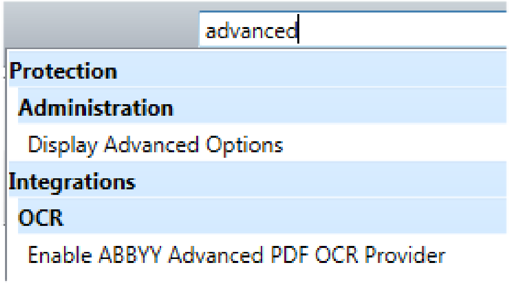

Workshare Configuration Manager (User Mode)
Workshare Configuration Manager
Launch Administrator Mode
Options
Licensing
Reset All To Default
Apply
Hide options I cannot change
Search Configuration Options
Protection
Administration
Secure File Transfer
Remove Metadata
Exclude Metadata
Convert to PDF
Compress as Zip
General
Administration
User Interface
Integrations
General
Help
Workshare Configuration Manager | Build 8.0.100.677 | Copyright ©1998-2013 Workshare Ltd.
Workshare

***Note**: In User Mode, the state of the options reflects the settings in HKEY_CURRENT_USER in the Registry.*

The configuration parameters for Workshare are grouped into categories and sub-categories. Click a sub-category to display the parameters for that sub-category. The different sub-categories and their parameters are described in *Workshare Configuration Options*.

Searching Parameters

If you know the name of a parameter (or part of its name) but not its location, you can search the Workshare Configuration Manager using the search box on the top right.



advanced

Protection

Administration

Display Advanced Options

Integrations

OCR

Enable ABBYY Advanced PDF OCR Provider

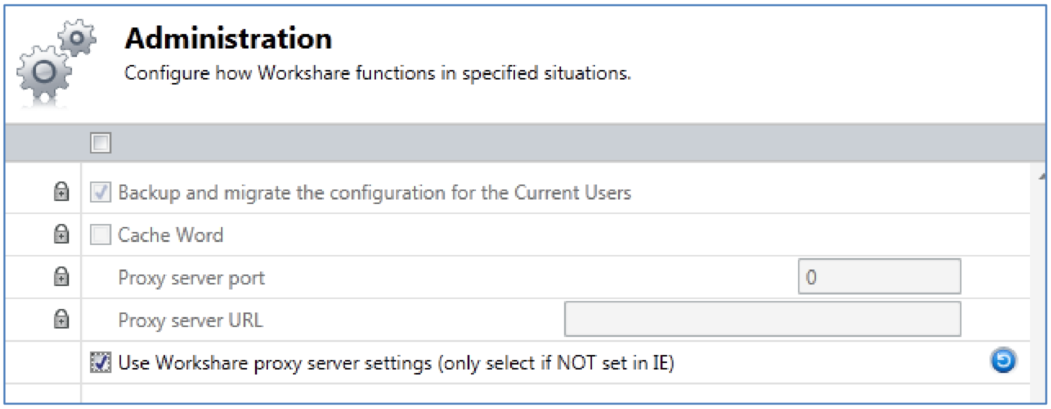
Click the parameter in the results list and the relevant category and sub-category is displayed in the Workshare Configuration Manager.

Setting Parameters

Most parameters in the Workshare Configuration Manager are set by selecting or deselecting a checkbox. There are also some that require you to enter a value in a text box.

To specify parameters:

1. In the Workshare Configuration Manager, select a category and then a sub-category.
2. Set a value for a parameter by selecting or deselecting the checkbox, selecting an option from a dropdown list or entering a value in a text box.



Administration

Configure how Workshare functions in specified situations.

☐

🔒 ☑ Backup and migrate the configuration for the Current Users

🔒 ☐ Cache Word

🔒 Proxy server port: 0

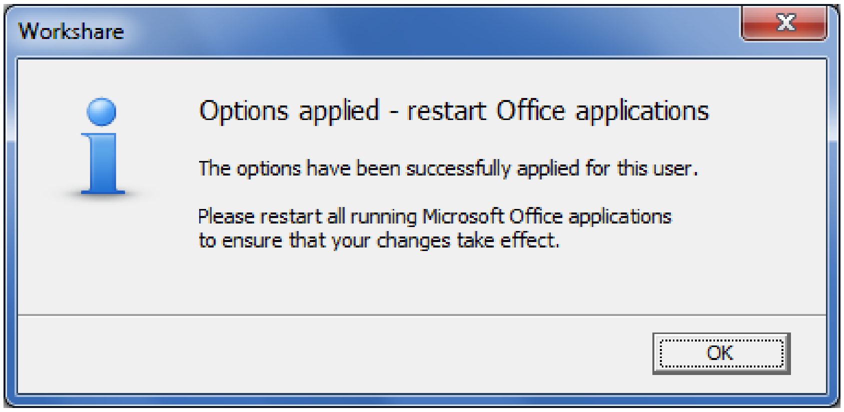
🔒 Proxy server URL:

☑ Use Workshare proxy server settings (only select if NOT set in IE) ↺

The ↺ icon to the right of a parameter indicates that the parameter value has been changed.

> ***Note**: When parameters have been locked by your administrator, the parameter will be disabled and a lock symbol will appear to the left of the parameter. You cannot change locked parameters.*

3. Continue to select categories and sub-categories and specify parameters as required.
4. Click **Apply** to save your settings. A confirmation message is displayed once the settings have been saved.



Workshare

Options applied - restart Office applications

The options have been successfully applied for this user.

Please restart all running Microsoft Office applications
to ensure that your changes take effect.

5. Click **OK** and restart all Microsoft Office applications.

> ***Note**: The different sub-categories and their parameters are described in Workshare Configuration Options.*

Appendix A. Clean and Lightspeed Clean

Lightspeed cleaning is a secure white-out technology that overwrites hidden data to prevent leaks. Lightspeed cleaning is much faster than regular cleaning because it does not rely on Microsoft Office for cleaning the document and uses exclusive binary reading and writing technology. Lightspeed cleaning maintains the original structure of the document but may either remove hidden data or redact it (replace it with spaces). Thus regular cleaning actually removes the hidden data element from the document whereas Lightspeed cleaning may have different effects. There are some subtle differences in how each technology cleans the document but both ensure the document is safe.

The following tables detail the features of Microsoft Word, Excel, PowerPoint and PDF documents that are cleaned by Workshare Protect when a **Clean** or a **Lightspeed Clean** is performed on the document. The tables also briefly explain the effect of the clean or Lightspeed clean. The effect of these actions varies according to the format of the document:

DOC/XLS/PPT	Word 97-2003 Document/Excel 97-2003 Workbook/PowerPoint 97-2003 Presentation
DOCX/XLSX/PPTX	Office Open XML Format (no macros)
DOCM/XLSM/PPTM	Office Open XML Format (macros allowed)
PDF	PDF or PDF/A

Microsoft Word Documents

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOCM Format	DOC Format	DOCX/DOCM Format
Track Changes	√ Deleted	√ Deleted	√ Deleted, but where track change deletes text, the text is turned into hidden spaces (revealed if turn on “show hidden text”)	√ Deleted
Comments	√ Deleted	√ Deleted	√ Deleted	√ Deleted
Small Text	√ Deleted	√ Deleted	√ Deleted, but turned into hidden spaces (revealed if turn on “show hidden text”)	√ Deleted
Color on Color Text (includes White Text)	√ Deleted	√ Deleted	√ Deleted, but turned into hidden spaces (revealed if turn on “show hidden text”)	√ Deleted

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOCM Format	DOC Format	DOCX/DOCM Format
Hidden Text	√ Deleted	√ Deleted	√ Deleted, but turned into hidden spaces (revealed if turn on “show hidden text”)	√ Deleted
Versions	√ Deleted	**NA**	√ Deleted	**NA**
Authors	√ Deleted	√ Deleted	√ Deleted	√ Deleted
AutoVersion	√ Cleared	**NA**	√ Cleared	**NA**
Custom Properties (in Custom tab)	√ Deleted	√ Deleted	√ Deleted	√ Deleted
Document Variables	√ Deleted	**X**	√ Name and value turned into spaces but the document variable still exists	√ Deleted
Macros	√ Deleted	√ Deleted	√ Deleted	√ Deleted
Routing Slip	√ Deleted	**NA**	√ Deleted	**NA**
Reviewers	√ Deleted	√ Deleted	√ Deleted	√ Deleted
Footnotes	√ Deleted	√ Deleted	√ Turned into hidden spaces (revealed if turn on “show hidden text”)	√ Deleted
Fields	√ Field code is deleted and the result turned to text	√ Field code is deleted and the result turned to text	√ Field code turned to blank spaces and the result left. When update performed, result becomes empty	√ Field code is deleted and the result turned to text

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOCM Format	DOC Format	DOCX/DOCM Format
Hyperlinks	√ Hyperlink removed and the result turned to text	√ Hyperlink removed and the result turned to text	√ Hyperlink turned to blank spaces and the result left. When update performed, result is error…	√ Hyperlink removed and the result turned to text
Document Statistics (in Statistics tab)	√ Deleted	X	√ Deleted “Last Saved By” and other fields reset.	√ Deleted “Last Saved By” and other fields reset.
Built-In Properties – Standard Properties (in Summary and Contents tabs)	√ Deleted	√ Deleted	√ Deleted “Title”	√ Deleted
Smart Tags	√ Deleted	√ Deleted	√ Deleted	√ Deleted
Template	√ Removes reference to template and shows only “Normal”	√ Removes reference to template and shows only “Normal”	√ Removes reference to template	√ Removes reference to template and shows only “Normal”
Headers	X	√ Checks headers in same way as body text	X	√ Checks headers in same way as body text
Footers	X	√ Checks footers in same way as body text	X	√ Checks footers in same way as body text
Endnotes	√ Deleted	√ Deleted	√ Deleted text of endnote but leaves separator	√ Deleted
Text Within Text Box	X	X	√ Deleted text from textbox	√ Deleted text from textbox

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOCM Format	DOC Format	DOCX/DOCM Format
SmartArt	X	X	√ Deleted	√ Deleted text from SmartArt

Microsoft Excel Workbooks

Feature	Clean		Lightspeed Clean	
	XLS Format	XLSX/XLSM Format	XLS Format	XLSX/XLSM Format
Track Changes	√	√	√	√
Comments	√	√	√ Comment turned to blank spaces but placeholder remains	√
Small Text	X	√	X	√
Color on Color Text (includes White Text)	X	√	X	√
Authors	√	√	√	√
Custom Properties (in Custom tab)	√	√	√	√
Macros	X	X	√	√
Routing Slip	√	NA	√	NA
Hyperlinks	X	X	√	√
Document Statistics (in Statistics tab)	√	X	√	√
Built-In Properties – Standard Properties (in Summary and Contents tabs)	√	√	√	√

Feature	Clean		Lightspeed Clean	
	XLS Format	XLSX/XLSM Format	XLS Format	XLSX/XLSM Format
Smart Tags	X	X	X	X
Headers	√	√	√	√
Footers	√	√	√	√
Text Within Text Box	X	X	X	X
SmartArt	NA	X	NA	X

Microsoft PowerPoint Presentations

Feature	Clean		Lightspeed Clean	
	PPT Format	PPTX/PPTM Format	PPT Format	PPTX/PPTM Format
Comments	√	√	√ Comment turned to blank spaces but placeholder remains	√
Small Text	X	X	X	X
Color on Color Text (includes White Text)	X	X	X	X
Authors	√	√	√	√
Custom Properties (in Custom tab)	√	√	√	√
Macros	X	X	√	√
Hyperlinks	X	X	√	√
Document Statistics (in Statistics tab)	X	√	√	X
Built-In Properties – Standard Properties (in Summary and Contents tabs)	√	√	√	√

Feature	Clean		Lightspeed Clean	
	PPT Format	PPTX/PPTM Format	PPT Format	PPTX/PPTM Format
Smart Tags	X	X	X	X
Template	X	X	X	X
Headers	X	X	X	√
Footers	X	X	X	√
Text Within Text Box	X	X	X	X
SmartArt	NA	X	NA	X
Speaker Notes	√	√	√	√
Hidden Slides	√	√	√	√

PDF Files

Workshare Protect does not distinguish between clean and Lightspeed clean when cleaning PDF files and whichever type of cleaning is selected, Workshare Protect will clean PDF files in the same way.

Feature	PDF	PDF/A
Attachments	√	√
Bookmarks	√	√
Markup	√	√
Properties	√	√ Cleaning Properties from PDF/A invalidates the PDF/A status