

# Workshare Protect User Guide

## Company Information

---

### Workshare Protect User Guide

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

Workshare Inc. (USA)  
208 Utah Street, Suite 350  
San Francisco  
CA 94103  
USA

Workshare Website: [www.workshare.com](http://www.workshare.com)

## Trademarks

Trademarked names appear throughout this guide as well as on other parts of the Workshare Protect CD. 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 the Workshare Protect User Guide and 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 the Workshare Protect User 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

© 2011. Workshare Ltd. All rights reserved. Workshare Professional and Workshare DeltaView are registered trademarks of Workshare Ltd. Workshare Compare, Workshare Protect, Workshare 3, Workshare DeltaServer, SafetyGain, and the Workshare logo are trademarks of Workshare Ltd. All other trademarks are those of their respective holders.

## Table of Contents

Chapter 1. Introducing Workshare Protect .....	6
What is Workshare Protect?.....	6
Workshare Protect Functionality .....	7
Discovering Content Risk.....	7
Manual Redaction.....	8
PDF Conversion .....	8
Document Classification .....	8
Chapter 2. Getting Started.....	9
Launching Workshare Protect .....	9
Start Menu .....	10
Batch Clean .....	10
Workshare Panel .....	10
Microsoft Word .....	11
Microsoft Excel and PowerPoint.....	12
Workshare Tab .....	12
Workshare Menu .....	14
Workshare Toolbar Buttons.....	14
Enabling Workshare Protect Functionality .....	15
Saved Documents .....	15
Latest Versions.....	16
Chapter 3. Managing Content Risk in Documents.....	17
Overview – Managing Content Risk in Documents.....	17
Displaying Content Risk in Microsoft Word .....	18
Displaying Content Risk in Microsoft Excel and PowerPoint.....	19
Cleaning Hidden Data .....	20
Batch Cleaning .....	21
Batch Cleaning Using a Command Line.....	24
Cleaning Options .....	25
Manual Redaction.....	29

Chapter 4. Protecting Email Attachments .....	31
Overview – Protecting Email Attachments .....	31
Protect Profile Dialog .....	32
Email Security Dialog.....	33
Using the Protect Profile Dialog .....	34
Using the Email Security Dialog.....	36
Password-Protected Documents .....	36
Send and Protect .....	38
Quick Tour of the Email Security Dialog.....	39
Select File Area .....	39
Summary Tab .....	40
Policies Tab .....	40
Other Tabs.....	40
Resolving Blocked Emails.....	41
Reviewing Alerts .....	42
Cleaning Hidden Data from Attachments.....	43
Converting Attachments to PDF .....	46
Chapter 5. Controlling Documents.....	49
Document Classification .....	49
Setting Classification Levels .....	50
Emailing Classified Documents.....	51
Chapter 6. Converting to PDF .....	54
Overview – Converting to PDF.....	54
Converting Documents to PDF.....	54
PDF and Emails.....	54
PDF Anywhere.....	54
Creating PDFs .....	55
Open Documents .....	55
Closed Documents.....	59
Creating PDFs and Sending by Email .....	59
PDF From Anywhere.....	60

Chapter 7. Configuring Workshare ..... 61

    Introducing the Workshare Configuration Manager ..... 61

        Administrator Mode and User Mode ..... 61

    Accessing the Workshare Configuration Manager ..... 61

        Searching Parameters ..... 63

        Setting Parameters ..... 63

**Appendix A.** Clean and Lightspeed Clean ..... 65

    Microsoft Word Documents ..... 65

    Microsoft Excel Workbooks ..... 68

    Microsoft PowerPoint Presentations ..... 69

# 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
- **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.

For users who have Workshare Device Protector (powered by Safend) or Safend Encryptor installed, Workshare Protect provides the following:

- **Monitoring and blocking content on USB and other removable media**

Safend policies define which files downloaded to external storage devices should be inspected and these files are then sent to the Workshare Protect client for inspection, where Workshare policy determines whether the files are blocked or the user alerted to sensitive information.

Refer to Safend Protector documentation for further details.

- **Full disk encryption**

Safend Encryptor provides a hard disk encryption solution that leverages the security of full-disk encryption and the flexibility of file-based encryption to protect sensitive data residing on desktops and laptops.

Refer to Safend Encryptor documentation for further details.

## 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).

***Note:** If Workshare is integrated with Workshare Device Protector (powered by Safend), Workshare offers enhanced content inspection for files transferred to removable media devices. Refer to the Safend Protector documentation for further information.*

## 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 (Portable Document Format). 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 added in Microsoft Office 2007/2010.
- **Workshare Menu**, page 14, describes the options available in the Workshare menu added in Microsoft Office 2003.
- **Enabling Workshare Protect Functionality**, page 14, 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, you see the following:

Microsoft Office 2003	Microsoft Office 2007/2010
In Microsoft Word, Excel and PowerPoint, the Workshare Panel is displayed down the left side of the window. Refer to Workshare Panel.	In Microsoft Word, Excel and PowerPoint, the Workshare Panel is displayed down the left side of the window. Refer to Workshare Panel.
In Microsoft Word, the <i>Workshare</i> menu is added to the menu bar. Refer to Workshare Menu.	In Microsoft Word, Excel and PowerPoint, the <i>Workshare</i> tab is added to the Ribbon. Refer to Workshare Tab.
In Microsoft Word, Excel and PowerPoint, Workshare buttons are added to the Standard toolbar. Refer to Workshare Toolbar Buttons.	

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.

**You can display/hide the Workshare Panel in any of the following ways:**

- MS Office 2007/2010: Click Toggle Panel in the Workshare tab, Options group.
- MS Office 2003: Select Show Workshare Panel from the Workshare menu (Microsoft Word only) or click the Toggle Workshare panel button  in the Standard Microsoft Word, Excel or PowerPoint toolbar.

The Workshare Panel 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.

## Microsoft Word

In Microsoft Word, 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!** In MS Office 2007, 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.

## Microsoft Excel and PowerPoint

In Microsoft Excel and PowerPoint, 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. Refer to Displaying Content Risk in Microsoft Excel and PowerPoint for further information.

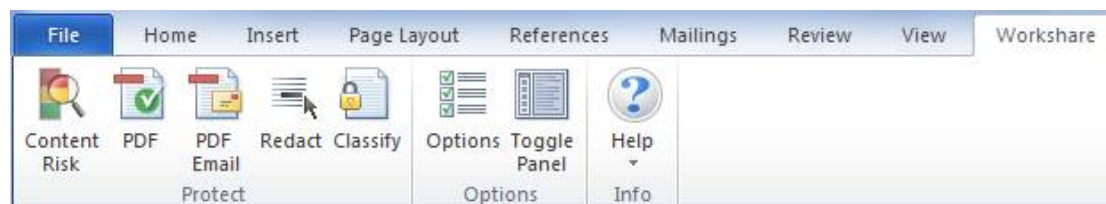
**PDF:** Enables you to convert documents to PDF. Refer to Overview – Converting to PDF for further information.

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

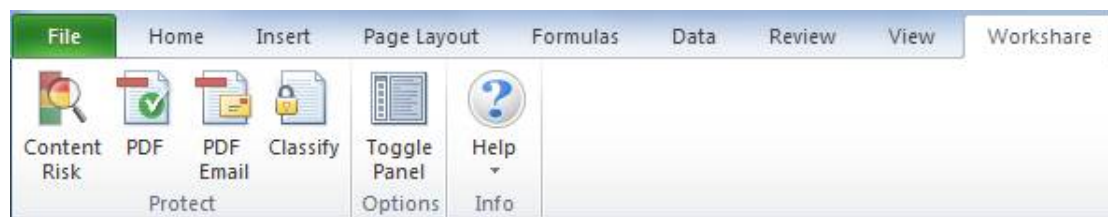
## Workshare Tab

The *Workshare* tab is available in Microsoft Office 2007/2010.

### 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.

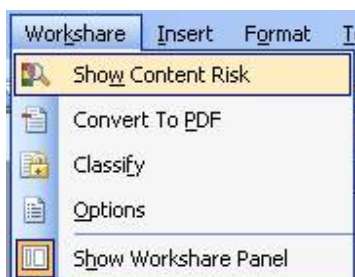
The *Workshare* tab includes the following options:

Group	Item	Description
<b>Protect</b>	<b>Content Risk</b>	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 <i>Displaying Content Risk in Microsoft Word</i> for further information.
	<b>PDF</b>	Enables you to convert documents to PDF. Refer to <i>Creating PDFs</i> for further information.
	<b>PDF Email</b>	Enables you to convert a document to PDF and adds the PDF as an attachment to an email. Refer to <i>Creating PDFs and Sending by Email</i> for further information.
	<b>Redact</b>	Enables you to redact/black out select text. Refer to <i>Manual Redaction</i> for further information.
	<b>Classify</b>	Enables you to classify your documents, which can restrict whether or not they can be emailed. Refer to <i>Document Classification</i> for further information.
<b>Options</b>	<b>Options</b>	Enables you to configure system parameters in the Workshare Configuration Manager. Refer to <i>Introducing the Workshare Configuration Manager</i> for further information.
	<b>Toggle Panel</b>	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 <i>Workshare Panel</i> .
<b>Info</b>	<b>Help</b>	Provides access to version, copyright and license information about Workshare Protect.

## Workshare Menu






The *Workshare* menu is available in Microsoft Word 2003. In Microsoft Office 2007/2010, functionality is available in the *Workshare* tab. Refer to Workshare Tab.

Whenever you open a document in Microsoft Word, the *Workshare* menu is included in the menu bar.







All of these menu items are configurable. It is also possible to replace the Workshare menu with a toolbar. This can be configured from the **General > User Interface** category in the Workshare Configuration Manager. Refer to *Workshare Configuration Options* for further information.

The *Workshare* menu includes the following options:

Menu Item	Toolbar Button	Description
<b>Show Content Risk</b>		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 Overview – Managing Content Risk in Documents for further information.
<b>Convert to PDF</b>		Enables you to convert documents to PDF. Refer to Creating PDFs for further information.
<b>Classify</b>		Enables you to classify your documents, which can restrict whether or not they can be emailed. Refer to Document Classification for further information.
<b>Options</b>		Enables you to configure system parameters in the Workshare Configuration Manager. Refer to Introducing the Workshare Configuration Manager for further information.
<b>Show Workshare Panel</b>		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.

## Workshare Toolbar Buttons

In Microsoft Office 2003, when Workshare Protect is installed, the following buttons are added to the **Standard** toolbar in Microsoft Word, Excel and PowerPoint:

	<b>Toggle Workshare panel</b>	Displays/hides the Workshare Panel.
	<b>Convert to PDF</b>	Enables you to convert a document to PDF.
	<b>Convert to PDF and email</b>	Enables you to convert a document to PDF and adds the PDF as an attachment to an email.
	<b>Redact selected text</b>	Enables you to redact/black out select text.

When you have selected to display the Workshare options in a toolbar, these buttons are included in the Workshare toolbar. To display the Workshare toolbar, select the **Replace Workshare menu with Workshare toolbar (Office 2003)** parameter (**General > User Interface** category) in the Workshare Configuration Manager and restart Microsoft Word.



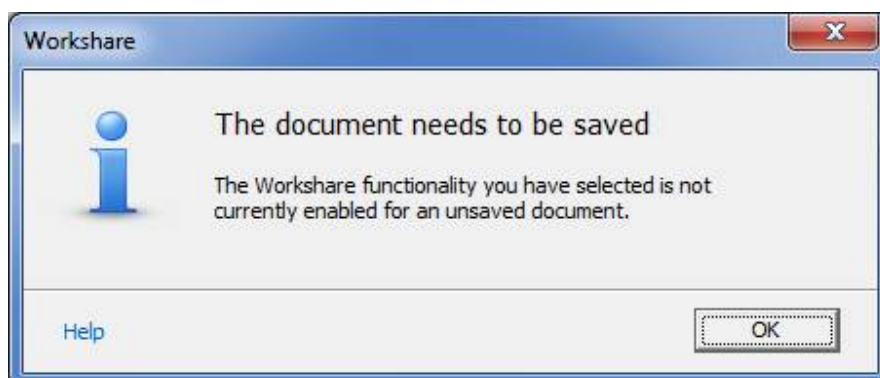
## Enabling Workshare Protect Functionality

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

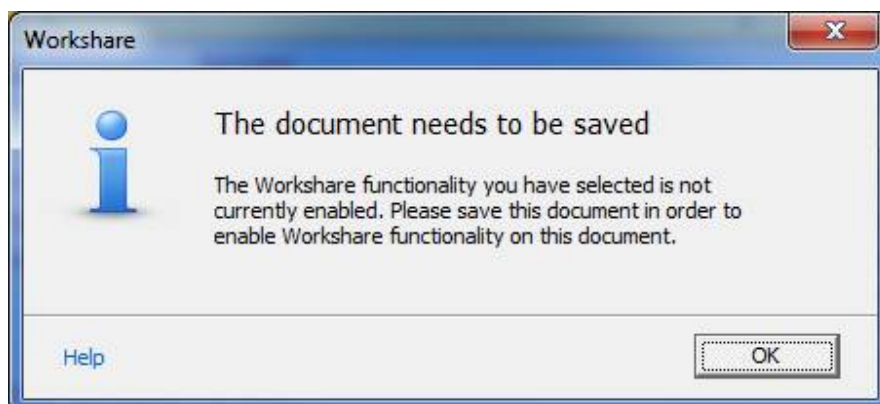
### Saved Documents

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:



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:



## Latest Versions

When you are working on a document in your DMS that is not the latest version, only the create PDF functionality is available. When you click **Content Risk** or **Classify**, the following message is displayed:



## 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 18, describes how to discover all content risk in a Microsoft Word document.
- **Displaying Content Risk in Microsoft Excel and PowerPoint**, page 19, describes how to discover all content risk in a Microsoft Excel or PowerPoint document.
- **Cleaning Hidden Data**, page 19, describes how to remove selected types of hidden data from a document and from multiple documents.
- **Manual Redaction**, page 29, 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. 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. 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

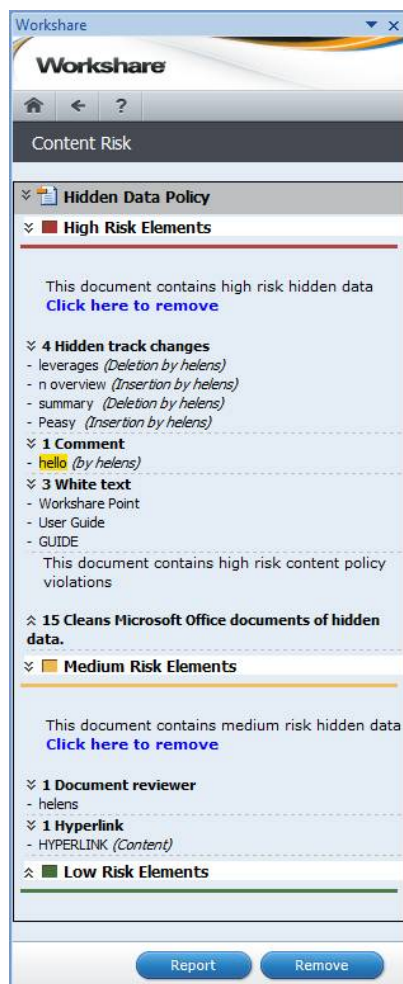
Workshare Protect integrates with Microsoft Word to provide an option to discover and view content risk in a document. You can also display a comprehensive report of all the content risk in a document.

### 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 from the *Workshare* menu, select **Show Content Risk**, 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.



Report

Remove

The content risk found is divided into high risk, medium risk and low risk (according to the risk level specified in the policy).

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.

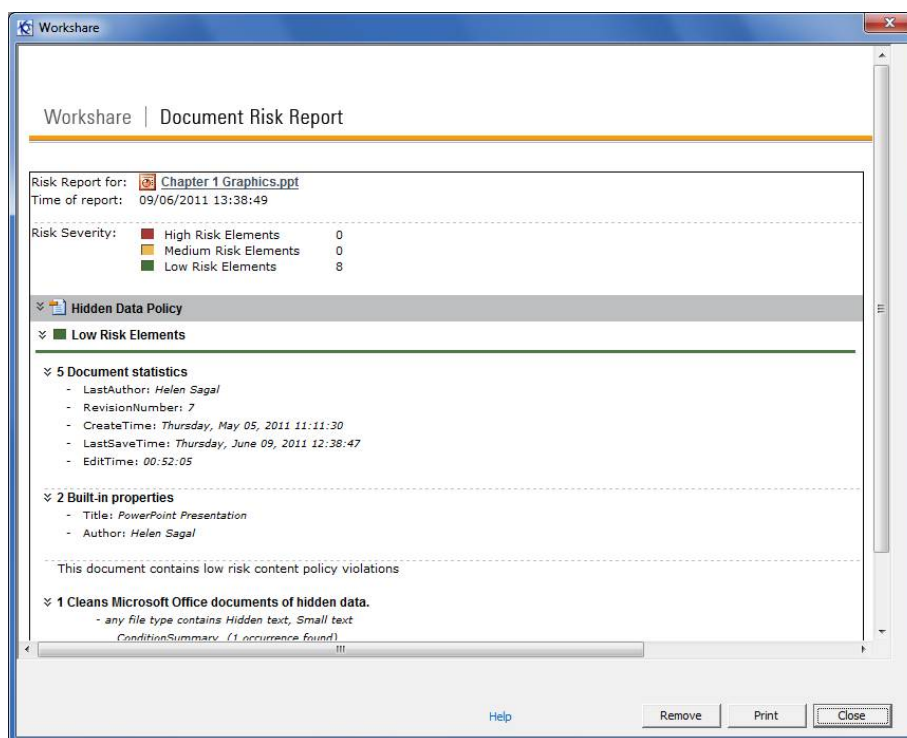
## Displaying Content Risk in Microsoft Excel and PowerPoint

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:



The content risk found is divided into high risk, medium risk and low risk (according to the risk level specified in the policy).

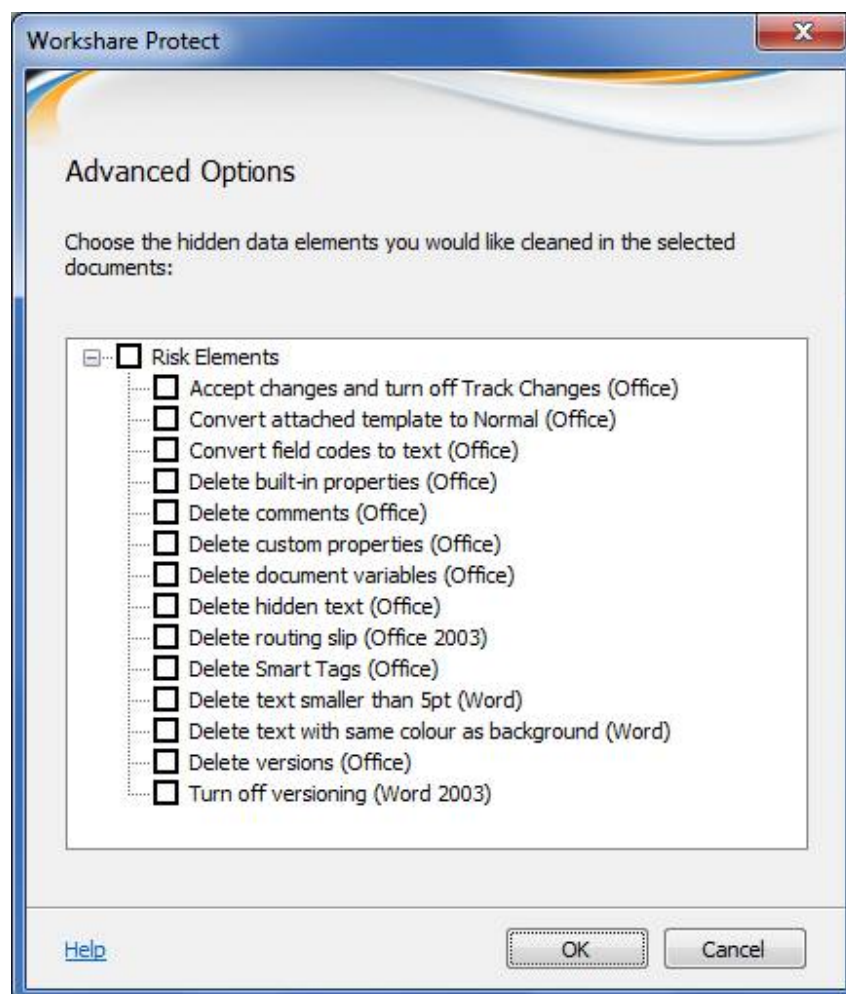
2. To print the report, click **Print**.
3. To remove the hidden data from the Microsoft Excel or PowerPoint document, click **Remove**. Refer to Cleaning Hidden Data for further information.

## 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 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.



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.

1. Select the hidden data you want to remove by selecting the checkboxes to the left of the hidden data options.
2. After making your selection, click **OK**. The selected hidden data is removed from the document.

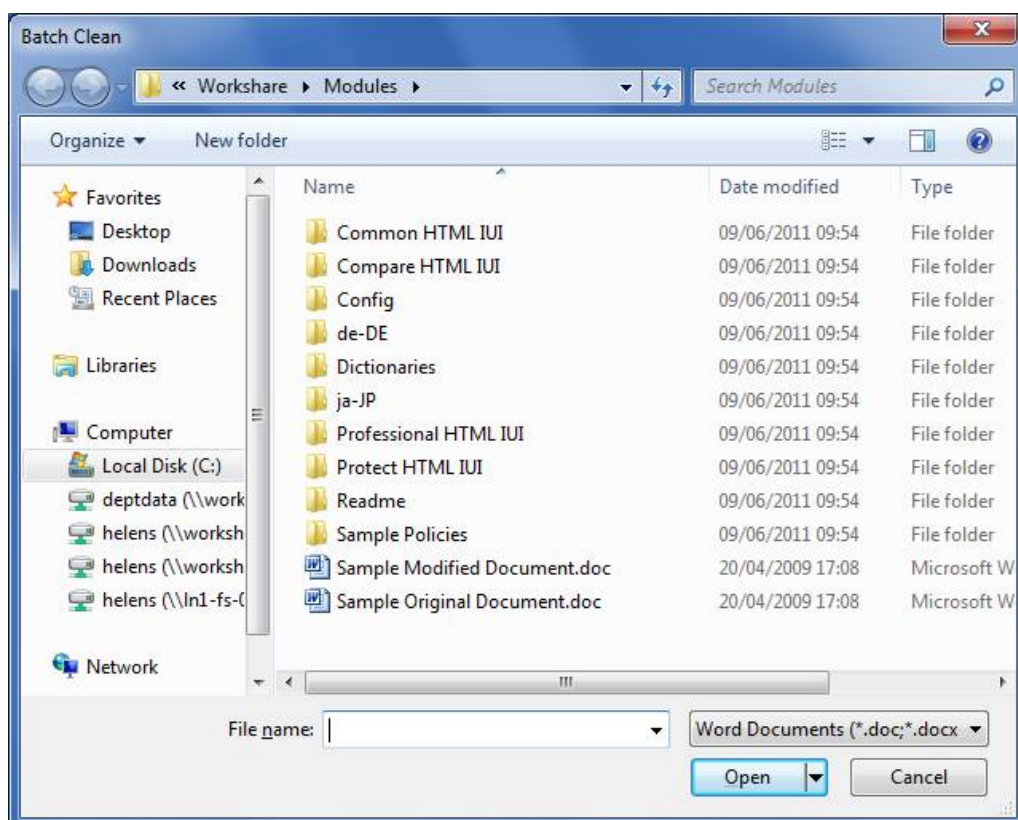
Workshare Protect may take a few moments to clean you document depending on the size of the document and the amount of hidden data to be removed. The Content Risk page/Document Risk Report is updated after the document has been cleaned to show any remaining content risk. After cleaning, the document 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:**

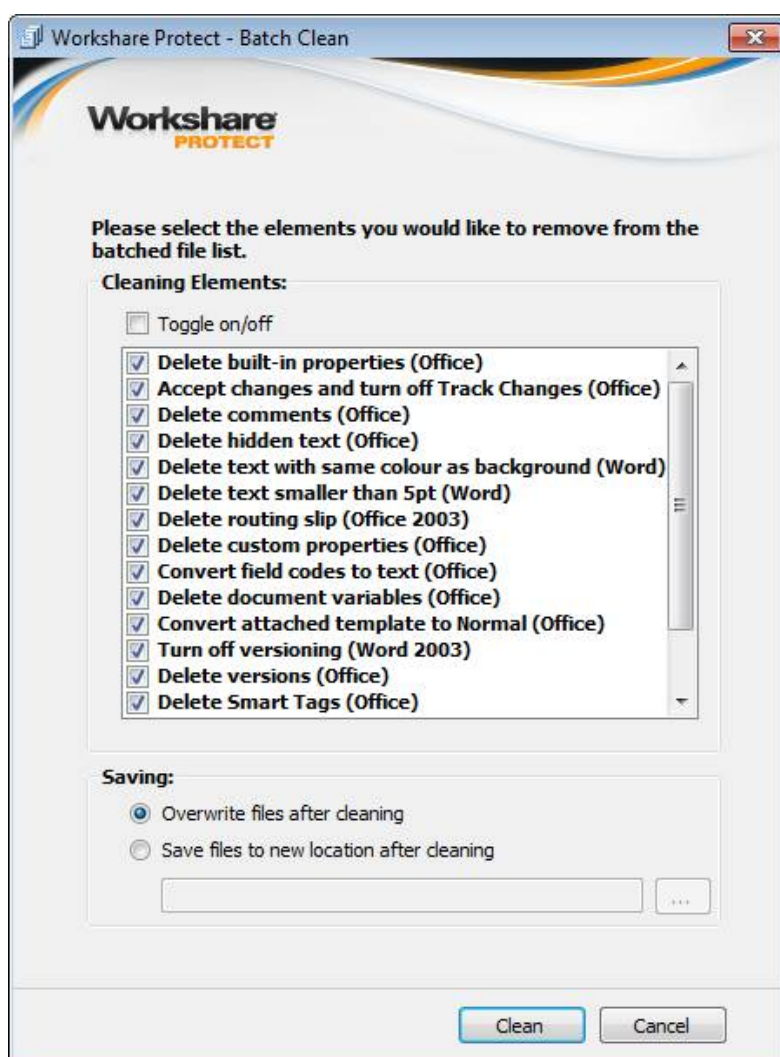
1. From the Start menu, select **Programs, Workshare**, and then **Workshare Batch Clean**. The *Batch Clean* dialog is displayed.



**Note:** To view more document types, select **All Office files** from the **Files of type** dropdown list. If non-supported 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**.

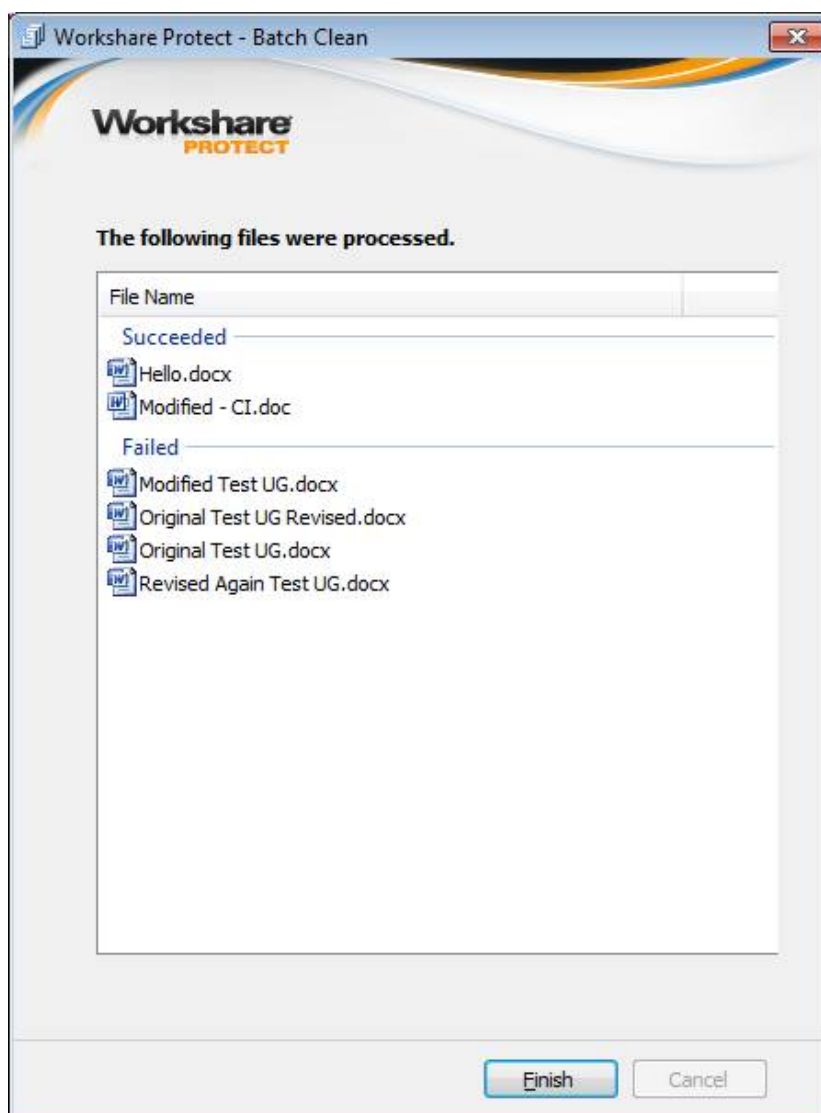


A complete list of hidden data that can be removed, reset or converted is listed in the dialog. For a full description of the different options, refer to *Cleaning Options*.

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

4. 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.
5. 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.



6. 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/
```

```
Administrator: C:\Windows\system32\cmd.exe
Workshare Protect Batch Cleaner 7.0.10000.0
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
/InstallShortcut     Installs SendTo link for current user only
/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:\Users\helens>
```

The options are described in the following table:

Option	Description
<code>/All</code>	All hidden data is removed from the specified documents. To leave specified types of hidden data in a document, the <code>/All</code> command can be used in conjunction with the <code>/Exclude</code> command. The <code>/All</code> command cannot be used in conjunction with the <code>/Include</code> command.
<code>/s</code>	Hidden data is removed from sub-folders of the specified folder.
<code>/WriteToFolder:[folder]</code>	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 <code>/WriteToFolder</code> command will have a flat file structure. If files have the same names, they will be appended with a number.
<code>/Exclude:[optionname]</code>	Excludes specified types of hidden data from being removed. The <code>/Exclude</code> command is used in conjunction with the <code>/All</code> command. The valid types of hidden data that can be excluded are detailed in the <b>optionnames</b> list.
<code>/Include:[optionname]</code>	Specifies which types of hidden data are to be removed. The <code>/Include</code> command is used instead of the <code>/All</code> command. The <code>/Include</code> command cannot be used with the <code>/All</code> command or the <code>/Exclude</code> command. The valid types of hidden data that can be specified are detailed in the <b>optionnames</b> list.
<b>optionnames</b>	The valid types of hidden data that can be used with the <code>/Exclude</code> and <code>/Include</code> 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
<b>Accept changes and turn off Track Changes (Word and Excel)</b>	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.

Option	Description
<b>Convert attached template to Normal (Word)</b>	<p>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.</p> <p>To view the attached template: In MS Word 2003, open the <i>Tools</i> menu and select <b>Templates and Add-Ins</b>. In MS Word 2007, click the Office Button, select <b>Word Options</b> and then select <b>Add-Ins</b>. From the <b>Manage</b> dropdown list, select <b>Word Add-ins</b> and click <b>Go</b>.</p>
<b>Convert field codes to text (Office)</b>	<p>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.</p> <p><i>Note: For Microsoft Excel and PowerPoint, hyperlinks are the only field codes that exist.</i></p> <p>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.</p> <p><i>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 Hidden Data Exclusions page of the Workshare Configuration Manager, and then clean field codes as normal. See Workshare Configuration Options for more details.</i></p> <p>To view field codes: In MS Word 2003, open the <i>Tools</i> menu and select <b>Options</b>. In the <b>View</b> tab, select the <b>Field Codes</b> checkbox in the <b>Show</b> area. In MS Word 2007, click the Office Button, select <b>Word Options</b> and then select <b>Advanced</b>. Select the <b>Show field codes instead of their values</b> checkbox in the <b>Show document content</b> area.</p>
<b>Delete built-in properties (Office)</b>	<p>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.</p> <p>To view built-in properties: In MS Office 2003, open the <i>File</i> menu and select <b>Properties</b>. In the <i>Properties</i> dialog, select the <b>Summary</b> and <b>Contents</b> tabs. In MS Office 2007, click the Office Button, select <b>Prepare</b> and then select <b>Properties</b>. In the Document Information Panel, select <b>Advanced Properties</b> from the <b>Document Properties</b> dropdown list. In the <i>Properties</i> dialog, select the <b>Summary</b> and <b>Contents</b> tabs.</p>

Option	Description
<b>Delete comments (Office)</b>	<p>Microsoft Word, Excel and PowerPoint. Removes any comments embedded in the document.</p> <p>To display comments: In MS Office 2003, open the Reviewing toolbar and from the <b>Show</b> dropdown list, select <b>Comments</b>. In MS Office 2007, click the <b>Review</b> tab and from the <b>Balloons</b> dropdown list (<b>Tracking</b> group), select <b>Show Only Comments and Formatting in Balloons</b>.</p>
<b>Delete custom properties (Office)</b>	<p>Microsoft Word, Excel and PowerPoint. Removes any custom properties that have been added to the document.</p> <p>To view document properties: In MS Office 2003, open the <i>File</i> menu and select <b>Properties</b>. In MS Office 2007, click the Office Button, select <b>Prepare</b> and then select <b>Properties</b>. In the Document Information Panel, select <b>Advanced Properties</b> from the <b>Document Properties</b> dropdown list. In the <i>Properties</i> dialog, select the <b>Custom</b> tab.</p>
<b>Delete document variables (Word)</b>	<p>Microsoft Word only. Deletes all document variables.</p> <p>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.</p> <p>Variables can be viewed in Microsoft Word in the Visual Basic Editor.</p>
<b>Delete hidden text (Word)</b>	<p>Microsoft Word only. Removes all text that has been formatted as hidden.</p> <p>To view hidden text: In MS Word 2003, from the <i>Tools</i> menu, select <b>Options</b>. Select the <b>View</b> tab and in the <b>Formatting marks</b> section, select the <b>Hidden Text</b> checkbox. In MS Word 2007, click the Office Button, select <b>Word Options</b> and then select <b>Display</b>. Select the <b>Hidden Text</b> checkbox.</p>
<b>Delete routing slip (Word and Excel 2003)</b>	<p>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.</p> <p>Routing slips are not supported in MS Office 2007.</p> <p>To view routing slip entries: From the <i>File</i> menu, select <b>Send To</b> and then <b>Routing Recipient</b>. To view envelope information: From the <i>File</i> menu, select <b>Send To</b> and then <b>Mail Recipient</b>.</p>

Option	Description
<b>Delete Smart Tags (Word)</b>	<p>Microsoft Word only. Removes smart tags from Microsoft Word documents.</p> <p>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.</p> <p>Smart tags only exist in Microsoft Office XP and later.</p> <p>To manage smart tags: In MS Word 2003, open the <i>Tools</i> menu and select <b>AutoCorrect Options</b>. Select the <b>Smart Tags</b> tab. In MS Word 2007, click the Office Button, select <b>Word Options</b> and then select <b>Proofing</b>. Click the <b>AutoCorrect Options</b> button and select the <b>Smart Tags</b> tab.</p>
<b>Delete text smaller than 5pt (Word)</b>	<p>Microsoft Word only. Removes all text that has been formatted with a font size less than 5pt (i.e. 4pt and less). Small text can also be detected in Microsoft Excel but it is not cleaned.</p> <p>To view small text: In MS Word 2003, from the <i>View</i> menu select <b>Zoom</b> and specify a percentage greater than 100%. In MS Word 2007, click the <b>View</b> tab, select <b>Zoom</b> and specify a percentage greater than 100%.</p>
<b>Delete text with same color as background (Word)</b>	<p>Microsoft Word only. Removes all text that has been formatted with the same font color as that of the background.</p> <p>To view such text: In MS Word 2003, from the <i>Tools</i> menu, select <b>Options</b>. Select the <b>General</b> tab and in the <b>General options</b> section, select the <b>Blue background, white text</b> checkbox. In MS Word 2007, click the <b>Page Layout</b> tab and select a color from the <b>Page Color</b> dropdown list (<b>Page Background</b> group).</p>
<b>Delete versions (Word 2003)</b>	<p>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.</p> <p>Document versions are not supported in MS Office 2007.</p> <p>To view versions: From the <i>File</i> menu, select <b>Versions</b>.</p>
<b>Turn off versioning (Word 2003)</b>	<p>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.</p> <p>Versioning is not supported in MS Office 2007.</p>
<b>Delete footers (Excel and PowerPoint)</b>	<p>Microsoft Excel and PowerPoint. Removes any footers included in the sheet or slide.</p> <p>To view headers and footers: In MS Excel and PowerPoint 2003, open the <i>View</i> menu and select <b>Header and Footer</b>. In MS Excel and PowerPoint 2007, click the <b>Insert</b> tab and select <b>Header &amp; Footer (Text group)</b>.</p>

Option	Description
<b>Delete headers (Excel and PowerPoint)</b>	Microsoft Excel and PowerPoint. Removes any headers included in the sheet or slide.  To view headers and footers: In MS Excel and PowerPoint 2003, open the <i>View</i> menu and select <b>Header and Footer</b> . In MS Excel and PowerPoint 2007, click the <b>Insert</b> tab and select <b>Header &amp; Footer (Text group)</b> .
<b>Delete links (Excel)</b>	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.
<b>Delete hidden slides (PowerPoint)</b>	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.
<b>Delete Speaker Notes (PowerPoint)</b>	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.

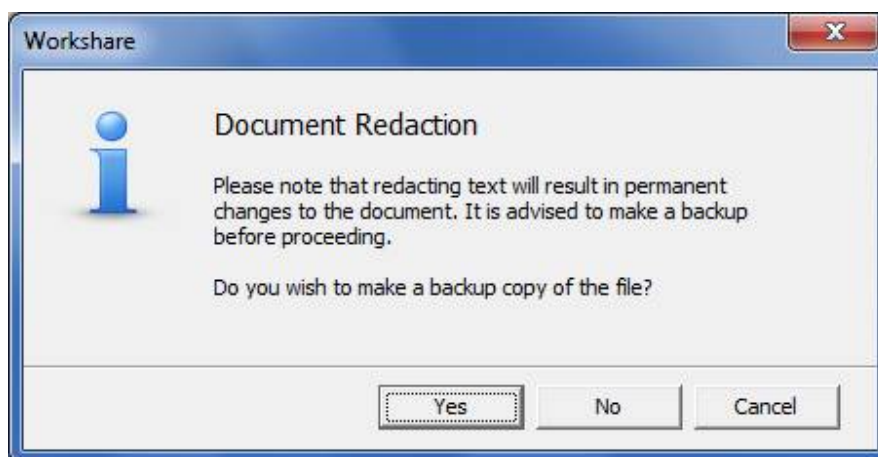
The functionality is available from a right-click menu and also from the Workshare tab (MS Word 2007) and Workshare toolbar (MS Word 2003).

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. Proceed in one of the following ways:
  - Right-click the selection and select **Redact Text**.
  - In MS Word 2003, click **Redact Selected** in the Standard toolbar or click **Redact Selected** in the Workshare toolbar.
  - In MS Word 2007, click **Redact** in the Workshare tab (**Protect** group).

The following message is displayed:



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]

**Note:** To display the Workshare toolbar, select the **Replace Workshare menu with Workshare toolbar (Office 2003)** parameter (**General > User Interface** category) in the Workshare Configuration Manager and restart Microsoft Word.

## Chapter 4. Protecting Email Attachments

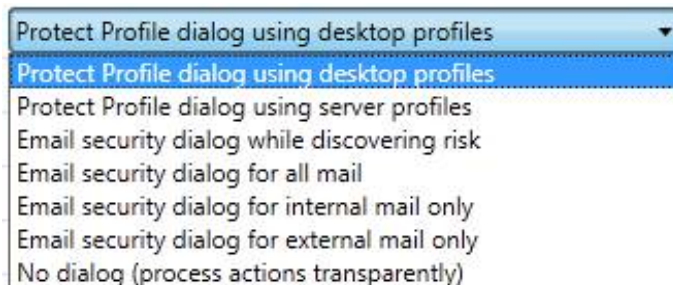
This chapter describes the Workshare Protect functionality with regard to identifying content risk in emails and their attachments. It includes the following sections:

- **Overview – Protecting Email Attachments**, below, introduces how Workshare Protect protects emails.
- **Using the Protect Profile Dialog**, page 34, describes how to send secure emails using the Workshare Protect Profile dialog.
- **Using the Email Security Dialog**, page 36, describes how to send secure emails using the Workshare Protect Email Security dialog.

### Overview – Protecting Email Attachments

Workshare Protect is able to process the emails you send and remove metadata from attachments or convert attachments to PDF. 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.

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).



When sending emails you may see the Protect Profile dialog or the Email Security dialog.

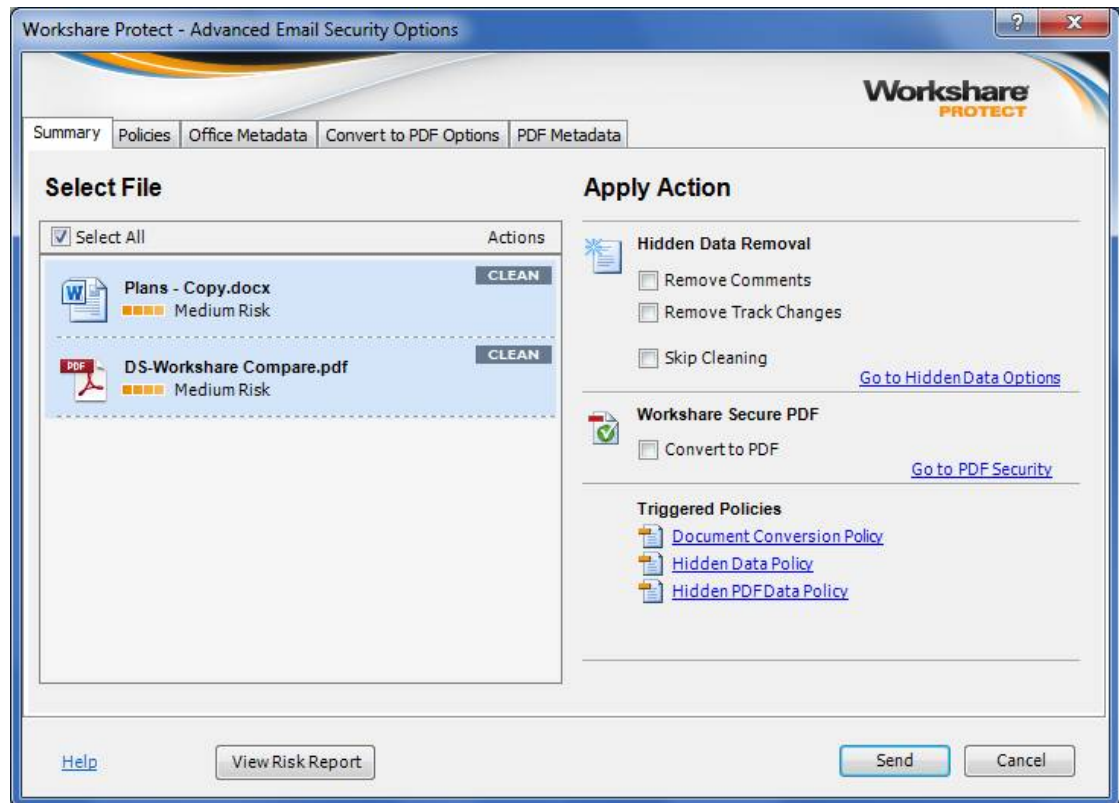
## Protect Profile Dialog



The Protect Profile dialog may be displayed in different ways depending on the option selected by your Administrator 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.

## Email Security Dialog



The Email Security dialog may be displayed in different circumstances depending on the option selected by your Administrator 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.

## 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 and whether to convert the attachment to PDF.

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.



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.

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 all options enabled. Refer to the next section for a description of the *Email Security* dialog.

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

## 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:** This action cleans the email and attached documents 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. This functionality is available as follows:

- MS Word 2003: From the *Tools* menu, select **Options** and in the *Options* dialog, select the **Security** tab.
- MS Word 2007 and above: Click the Office button and select **Save As**. From the *Save As* dialog, click **Tools** and select **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,



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. This functionality is available as follows:

- MS Word 2003: From the *Tools* menu, select **Protect Document**.
- MS Word 2007 and above: In the **Review** tab, click **Protect Document**.

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



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.

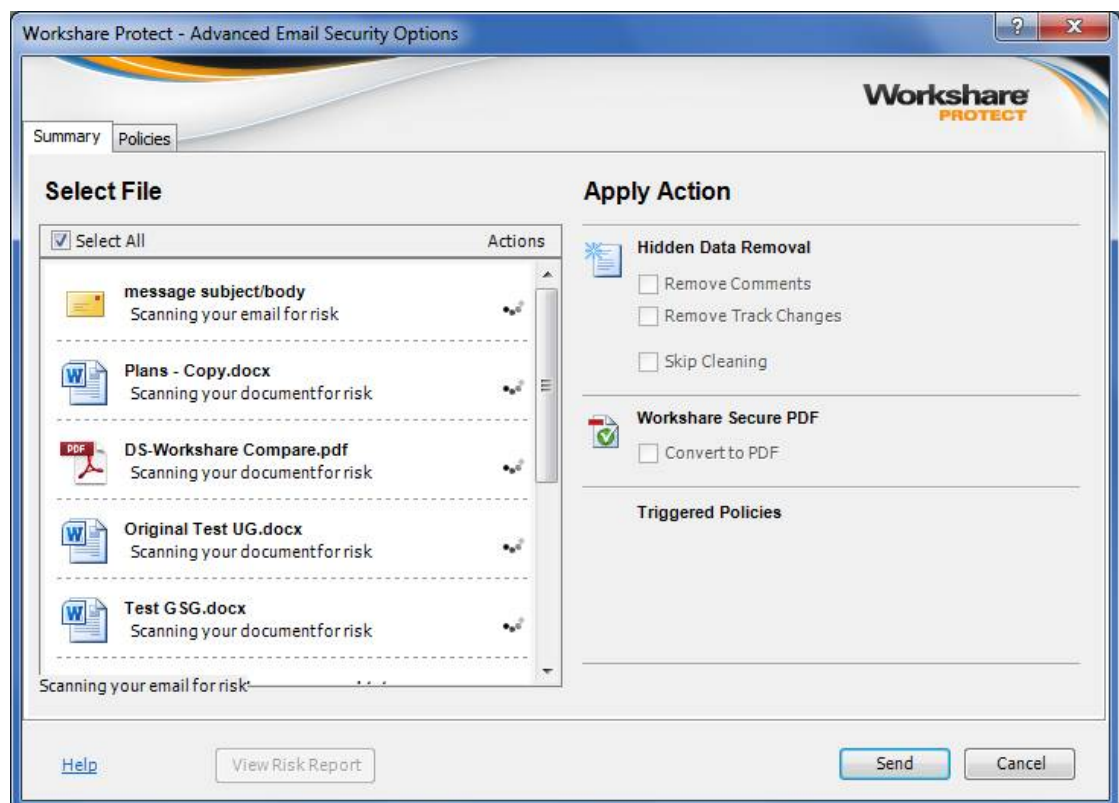
## Send and Protect

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.

### 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 (*After an email with attachments is sent 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.



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 to the settings in the default profile. This means 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.

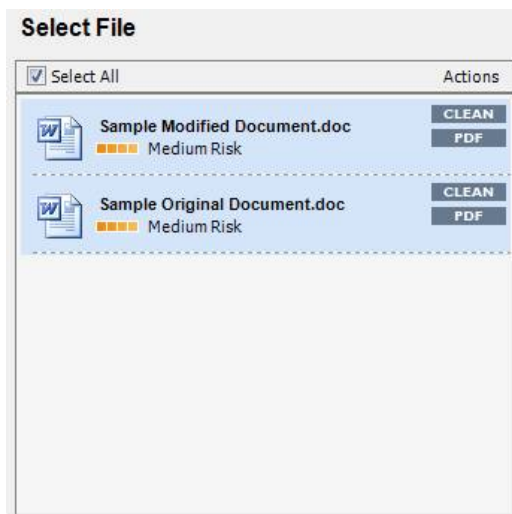
## Quick Tour of the Email Security Dialog

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.



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**

**Hidden Data Removal**

- Remove Comments
- Remove Track Changes
- Skip Cleaning

[Go to Hidden Data Options](#)

**Workshare Secure PDF**

- Convert to PDF

[Go to PDF Security](#)

**Triggered Policies**

- [Document Conversion Policy](#)
- [Hidden Data Policy](#)

Under **Hidden Data Removal**, selecting **Remove Comments** or **Remove Track Changes** cleans comments or track changes from the selected attachment. Selecting **Skip Cleaning** means the selected attachment is not cleaned at all.

Under **Workshare Secure PDF**, selecting **Convert to PDF** means the selected attachment is converted into PDF.

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 its attachments.

**View Policies**

**Hidden Data Policy** [\[ Less \]](#)

Clean policy.

**Based on the following routing:**  
To External Recipients

**The following has triggered the policy:**  
Cleans Microsoft Office documents of hidden data.

**Why is this important?**

**Document Conversion Policy** [\[ More \]](#)

[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* for more information.

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

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

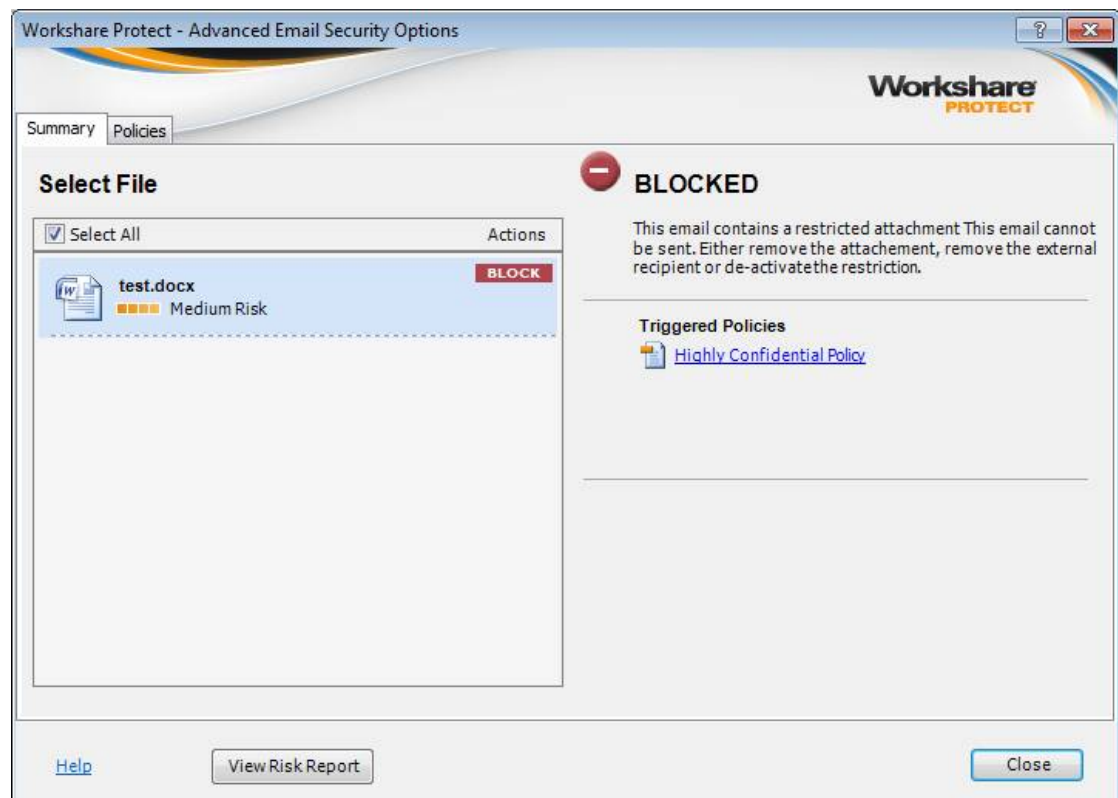
The **ZIP Options** tab is included in the *Email Security* dialog when a Zip action is triggered.

## 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.



### 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.

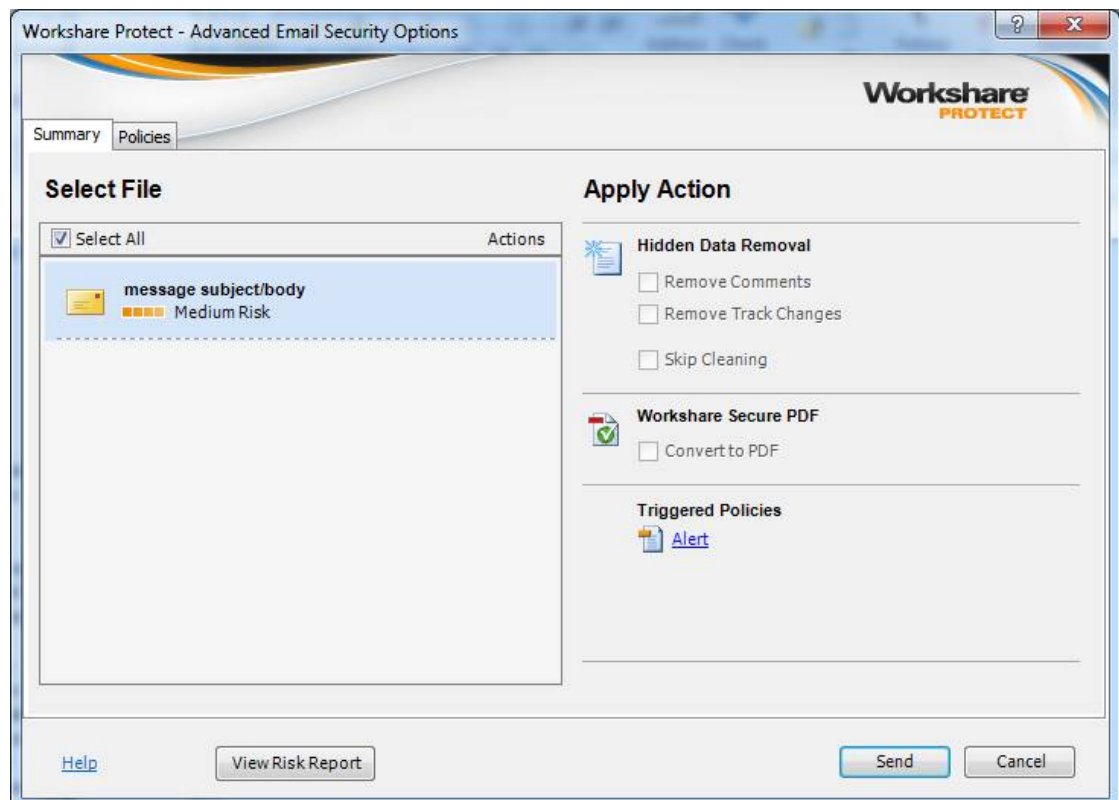
2. Click the **Close** button to close the *Email Security* dialog.
3. Make the appropriate changes to the email and/or document(s) by removing or modifying the content, attachments or recipients that caused your email to be blocked.
4. If making changes to attachments, re-attach the corrected documents.
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.



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** and **Lightspeed Clean** actions remove hidden data, such as track changes, hidden text, comments, 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** or a **Lightspeed Clean** action, Workshare Protect notifies you that your email and/or attachment(s) will be cleaned.

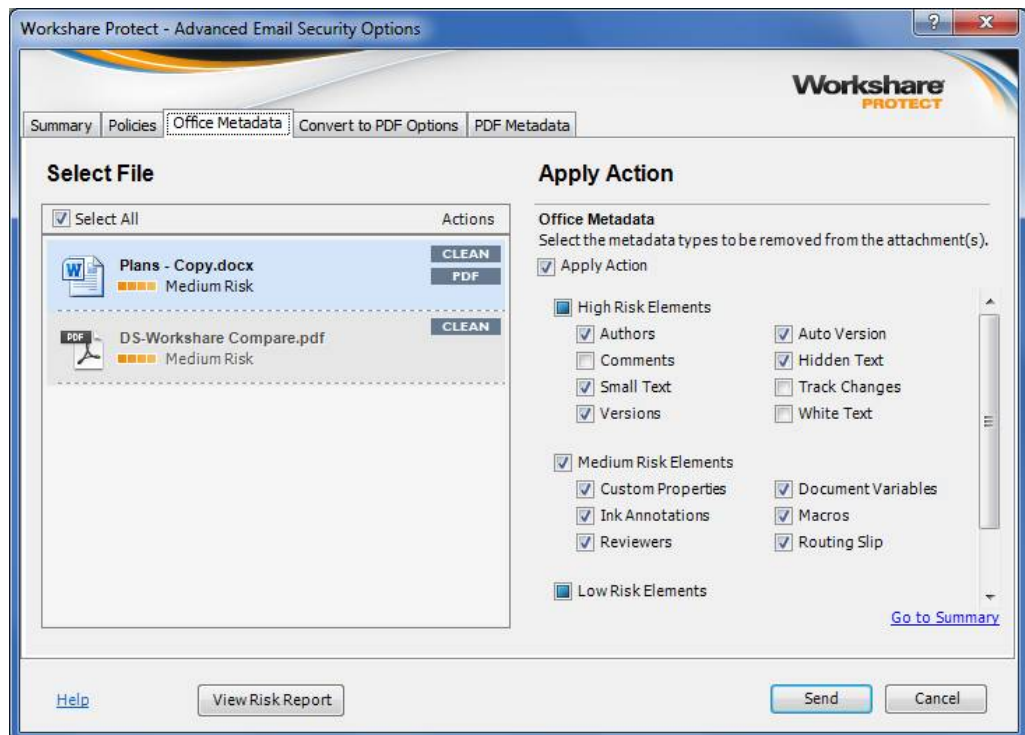
The screenshot displays the 'Workshare Protect - Advanced Email Security Options' dialog box. The 'Summary' tab is active, showing a list of files to be processed. Two files are listed: 'Plans - Copy.docx' (Medium Risk) and 'DS-Workshare Compare.pdf' (Medium Risk). Each file has a 'CLEAN' button next to it. The 'Apply Action' section on the right allows for configuring security actions. Under 'Hidden Data Removal', there are checkboxes for 'Remove Comments', 'Remove Track Changes', and 'Skip Cleaning'. Under 'Workshare Secure PDF', the 'Convert to PDF' checkbox is checked. The 'Triggered Policies' section lists three policies: 'Document Conversion Policy', 'Hidden Data Policy', and 'Hidden PDFData Policy'. At the bottom of the dialog, there are buttons for 'Help', 'View Risk Report', 'Send', and 'Cancel'.

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

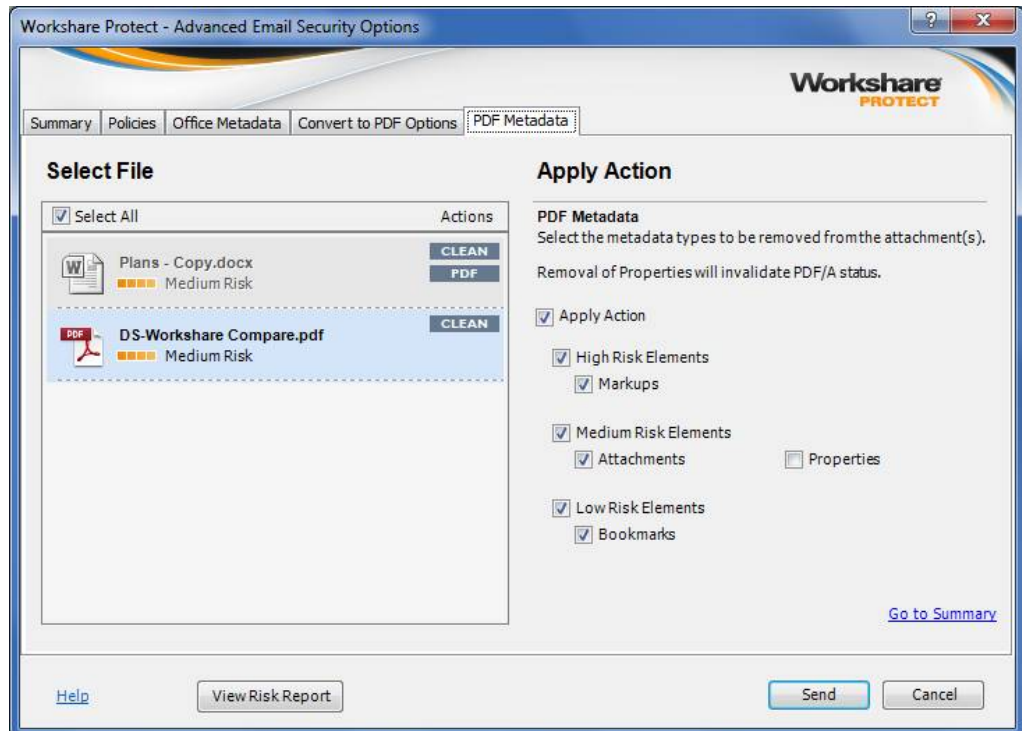
If your administrator has enabled you to override the clean hidden data settings and you do not want to clean the attachment(s), you can select the **Skip Cleaning** checkbox in the **Apply Action** area.

**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 **Go to Hidden Data Options** in the **Apply Action** area or select the **Hidden Data Options** tab. The **Hidden Data Options** tab displays the different hidden data cleaning options for Microsoft Office attachments.



3. Select the **PDF Metadata** tab to display the different hidden data cleaning options for PDF attachments.



**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.

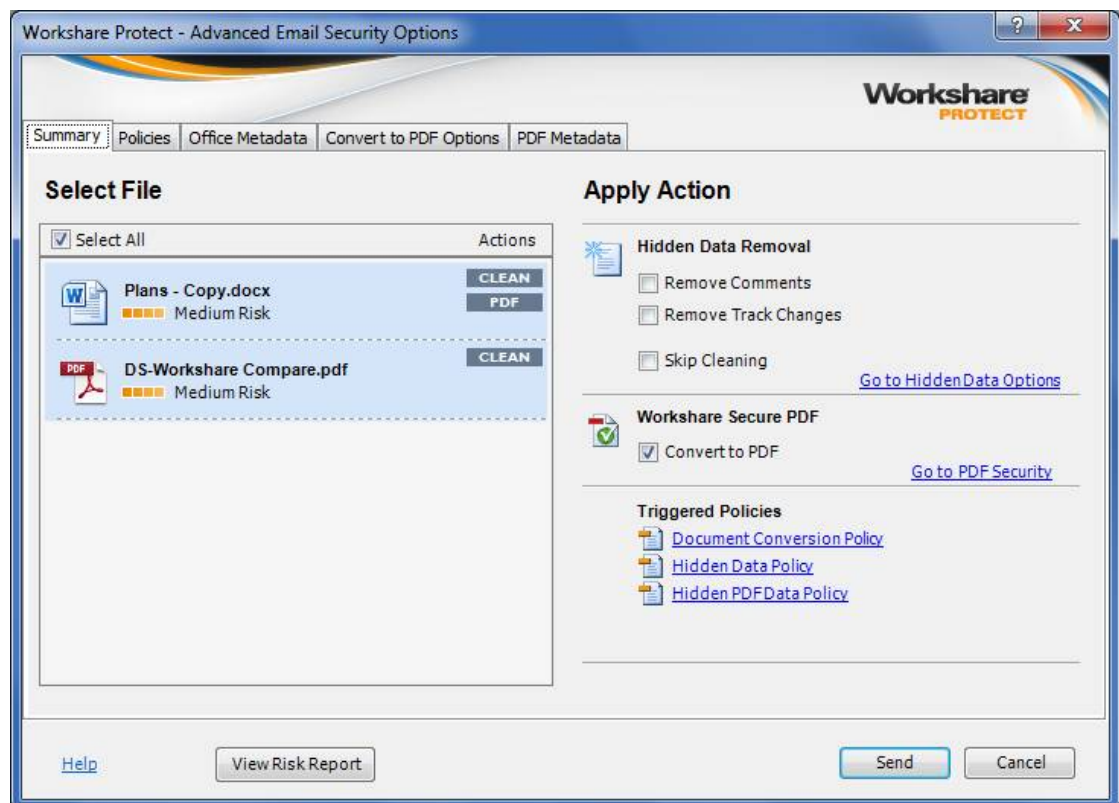
Workshare Protect cleans the hidden data from the attached document(s) according to your settings before sending the email.

## 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.

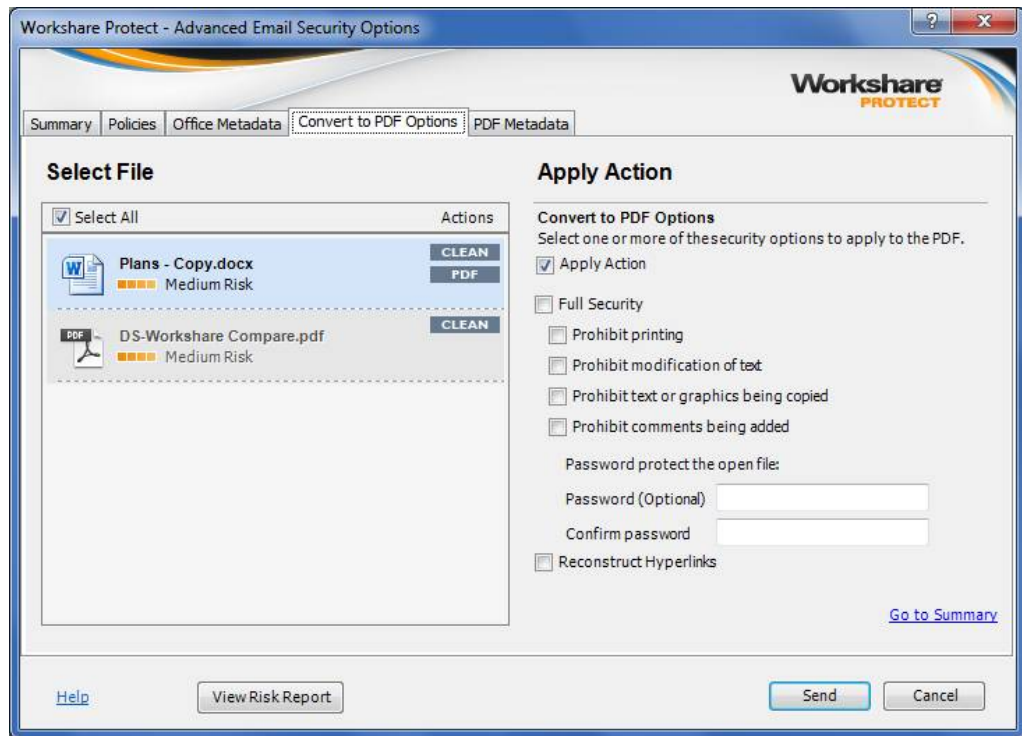
When you send an email that triggers a **PDF** action, Workshare Protect notifies you that your attachment(s) will be converted to PDF.



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 **Go to PDF Security** in the **Apply Action** area or select the **Convert to PDF Options** tab. The **PDF Options** tab displays the different PDF security settings available.



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

2. Select one or more of the security options individually or select the **Full Security** checkbox to select them all. The security options are:
  - **Prohibit printing** to prevent recipients from printing the PDF document.
  - **Prohibit modification of text** to prevent recipients with Adobe Distiller from editing the PDF document.
  - **Prohibit text or graphics being copied** to prevent recipients from copying graphics or text directly from the PDF document.
  - **Prohibit 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 **Prohibit comments being added** as well as **Prohibit modification 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. Repeat steps 2 to 4 for additional attachments if required.
6. Click **Send** to send the email.

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

## 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 50, describes how to classify a document.
- **Emailing Classified Documents**, page 51, 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 behaviour.*

- **Highly Confidential:** The document contains information of a highly confidential nature and when emailed wither 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 behaviour.*

- **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 from the *Workshare* menu, select **Classify**, or click **Classify** in the Home page of the *Workshare Panel*. The Document Classification page is displayed.



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 wither 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.

The screenshot shows a dialog box titled "Workshare" with a close button (X) in the top right corner. The main text reads: "Please enter the password and confirmation of the password to protect the Document Restrictions." Below this text are two input fields: "Password:" and "Confirm:". At the bottom of the dialog, there is a "Help" link on the left and "OK" and "Cancel" buttons on the right.

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

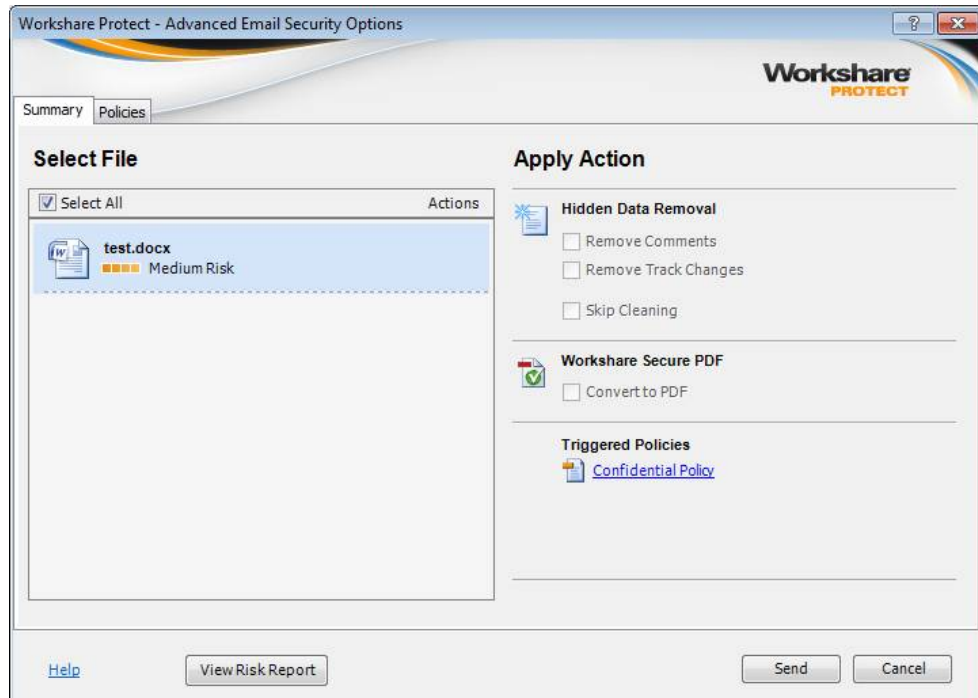
5. Enter the password twice to set and confirm the password and click **OK**.
6. Save the document. The open document is now restricted according to the selected classification level.

## Emailing Classified Documents

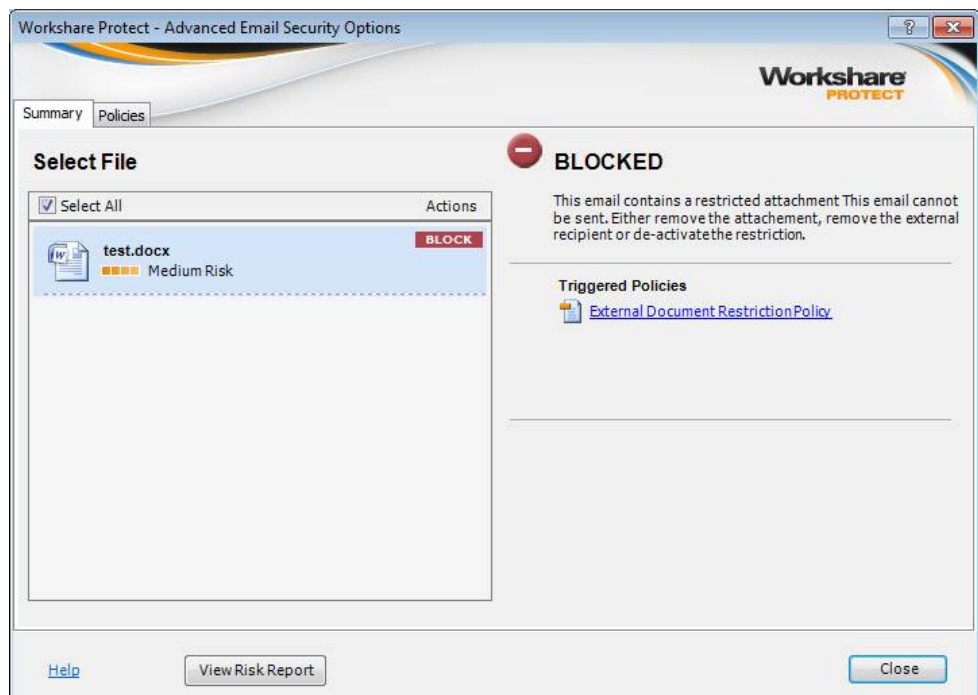
When a document is emailed, the classification level is checked and the document is handled according to its classification level:

- 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**.

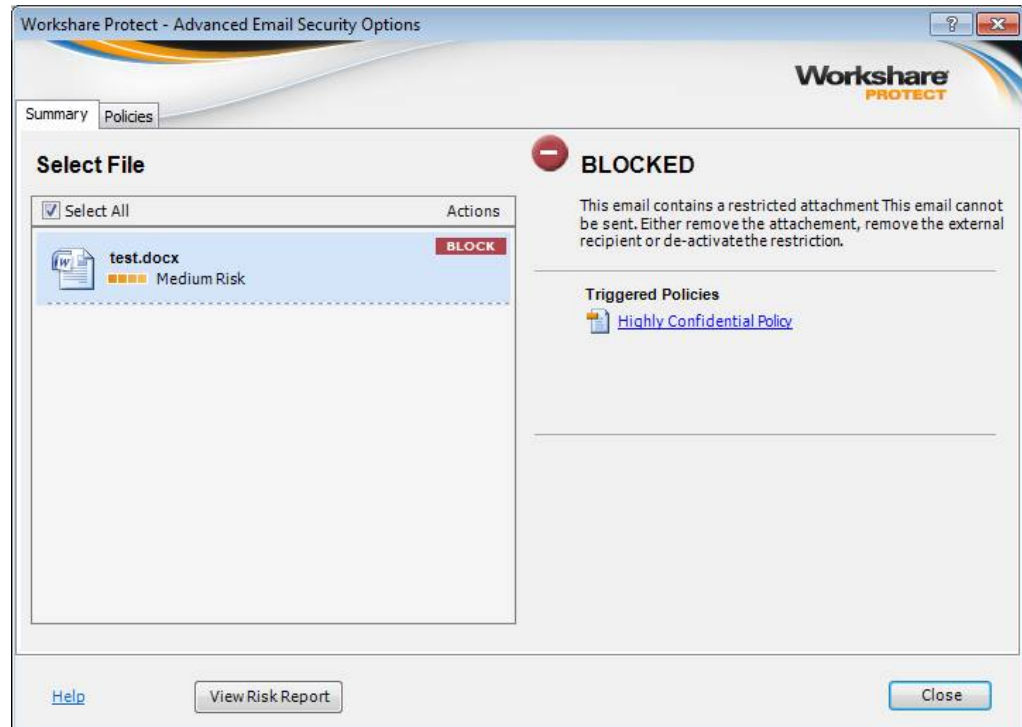


- If the document has a **For Internal Use** or **External Restriction** classification, it can be freely emailed to internal recipients. However, if you try to email it to an external recipient, the following dialog is displayed:



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.



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 55, describes how to convert a document to PDF.
- **Creating PDFs and Sending by Email**, page 59, describes how to convert a document to PDF and send by email.
- **PDF From Anywhere**, page 60, 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. You can also enforce PDF creation on email attachments leaving your organization. When sending documents for review, you can convert to PDF 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). 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 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 and Sending by Email.

### 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. 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. Documents can be stored locally, in SharePoint or in your DMS.

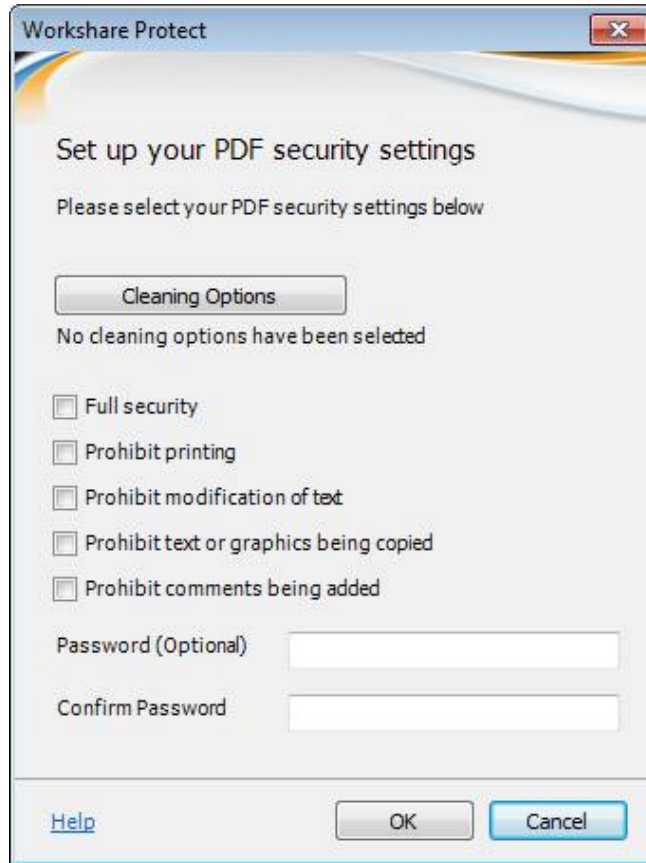
### To convert an open document to PDF:

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

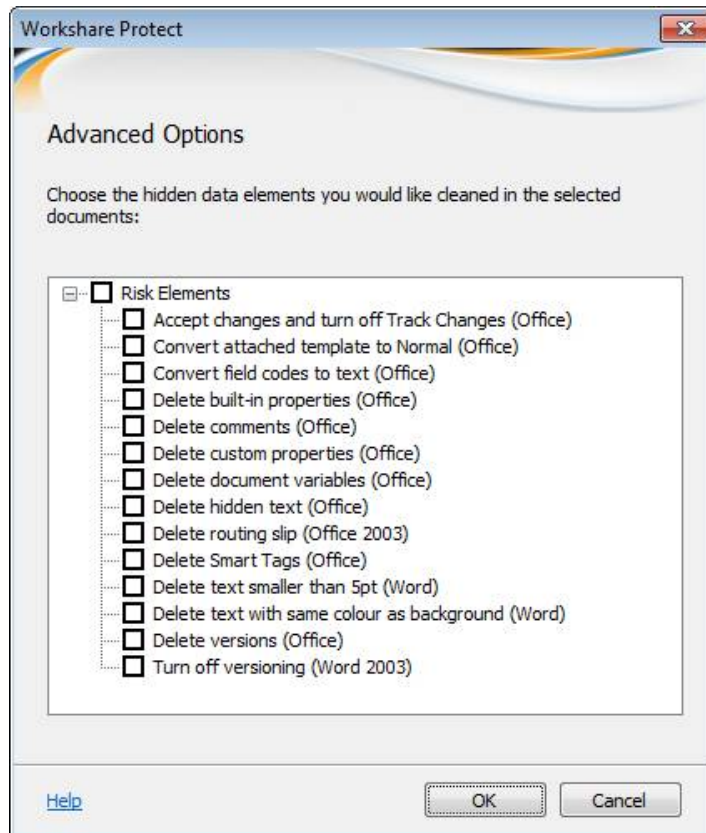


**Note:** The *Print* range area is slightly different in Microsoft Excel and PowerPoint.

2. If required, you can click the **PDF Security Options** link to set PDF security options. The PDF Security Settings dialog is displayed



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

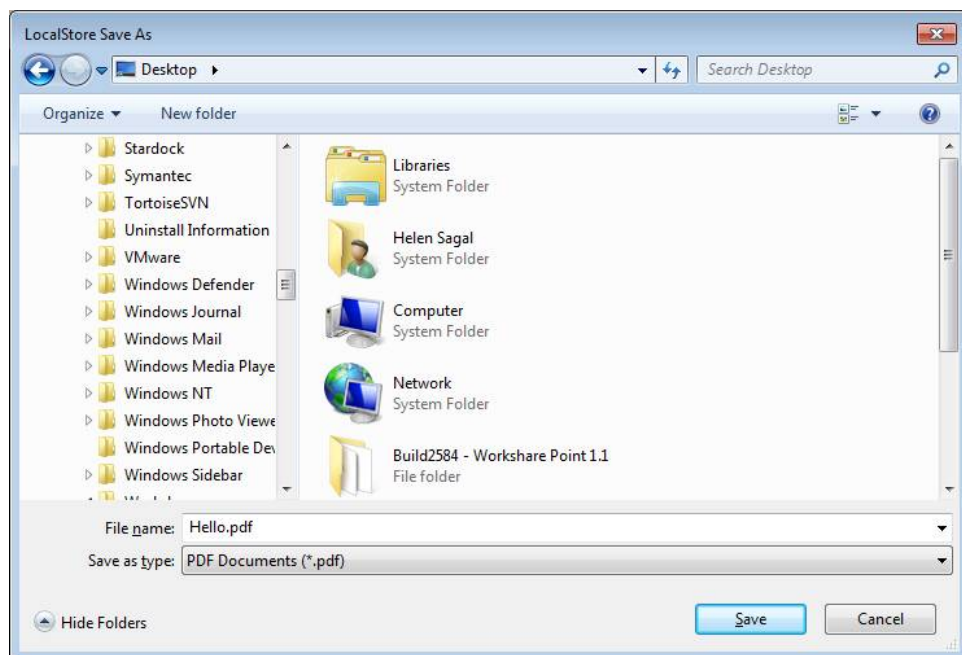


4. Select hidden data elements as required. For a full description of all the hidden data elements, refer to [Cleaning Hidden Data](#) for further information.
5. Click **OK**.
6. In the PDF Security Settings dialog, select one or more of the security options individually or select the **Full security** checkbox to select them all. The security options are as follows:
  - **Prohibit printing:** Prevents recipients from printing the PDF document.
  - **Prohibit modification of text:** Prevents recipients with Adobe Distiller from editing the PDF document.
  - **Prohibit text or graphics being copied:** Prevents recipients from copying graphics or text directly from the PDF document.
  - **Prohibit comments being added:** Prevents recipients with Adobe Distiller from adding comments to the PDF document.
7. If required, set a password to protect the PDF by entering the password twice in the relevant fields. When a password is specified, the recipient can only open the PDF after entering this password.
8. Click **OK**.

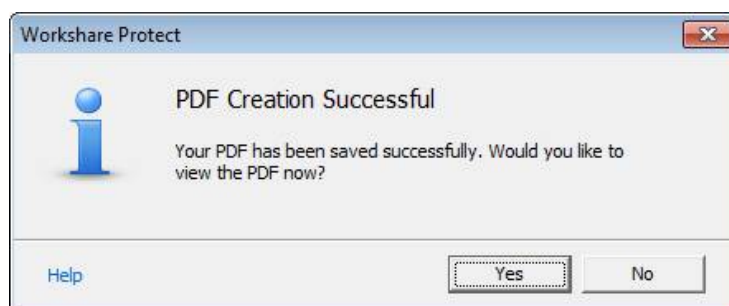
9. In the *Convert to PDF* dialog, if you want to create a PDF of part of the document only, select the **Pages** radio button and specify a page range. From the **Print** dropdown list, you can then select whether to PDF all pages in the specified range or only the odd or even pages.

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

10. If required, click **Preview** to view the document as a PDF.
11. Click **OK**. A Save dialog is displayed:



12. Specify the name and location for the PDF file and click **Save**. The document is converted to PDF. When the process is complete, the following message is displayed:



13. Click **Yes** to open the PDF file. If you click **No**, you can open the PDF at any later time from the save location.

## Closed Documents

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

### To convert a closed document to PDF:

1. 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.
2. Continue as described in steps 2 to 13 of the Open Documents section.

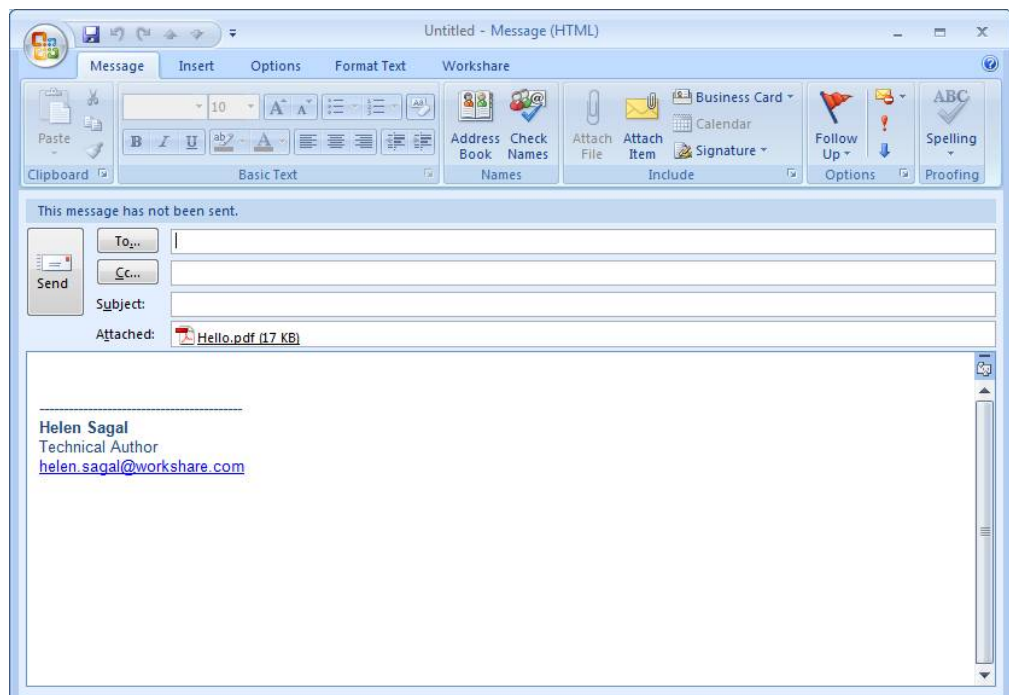
## Creating PDFs and Sending by Email

At any time when working on a document in Microsoft Word, Excel or PowerPoint, you can convert the document into PDF and send it by email.

### To create a PDF and send by email:

1. With your document open in Microsoft Word, Excel or PowerPoint, click **PDF Email (Protect group)** in the Workshare tab, or from the *Workshare* toolbar, click **Convert to PDF and Email**. The *Convert to PDF* dialog is displayed.
2. Follow the procedure to create a PDF as described in steps 2 to 12 of the *Creating PDFs* section.

After specifying a save location and clicking **Save**, an email message window is displayed with a PDF of the open document as an attachment.



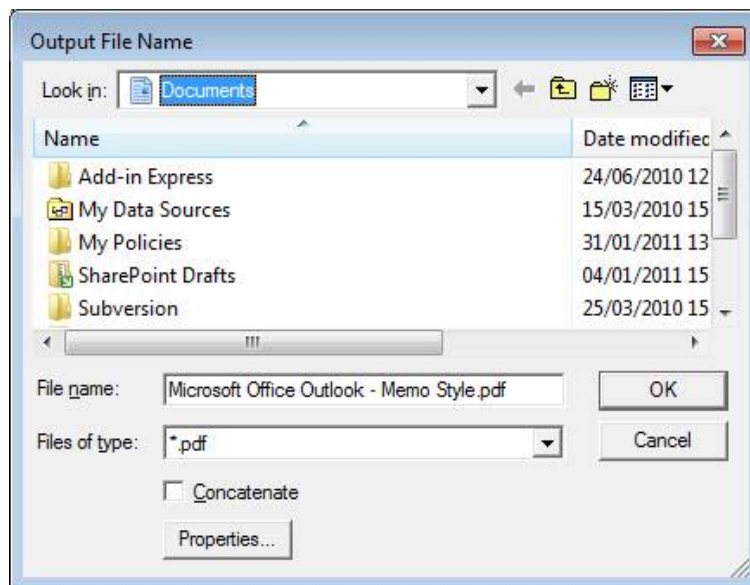
3. Enter the recipient(s) name and any other text you want to include and click **Send**. The PDF document is sent to the specified recipients.

## 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. In the *Print* dialog, select **Workshare PDF Publisher** as the printer.
3. Specify other settings as required and click **Print**. The *Output File Name* dialog is displayed.



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 63, 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 or from the *Workshare* menu, select **Options**. 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.

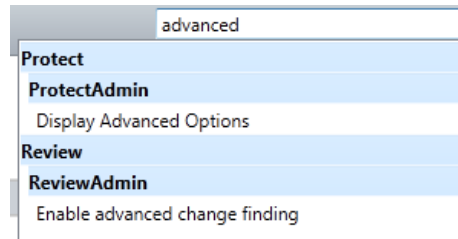


**Note:** In User Mode, the state of the options reflects the settings in `HKEY_CURRENT_USER` in the Registry.

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.



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 documents are displayed in Workshare Compare as well as how Workshare Compare functions in specified situations.

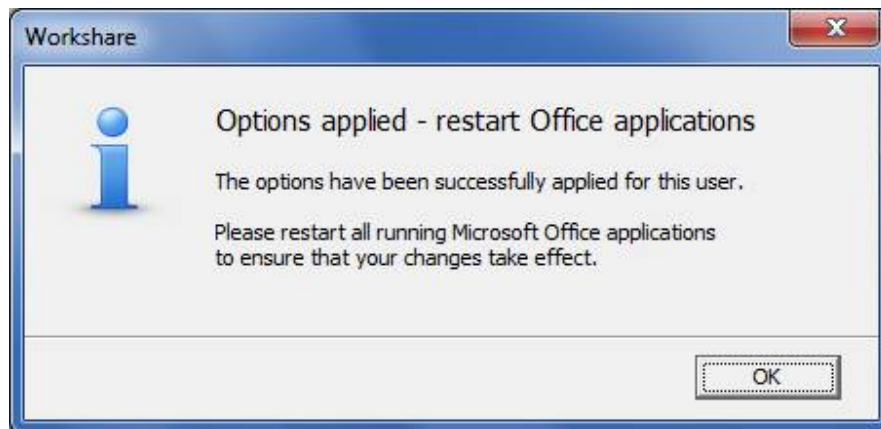
---

<input type="checkbox"/>	Additional locations for rendering sets	<input type="text"/>
<input type="checkbox"/>	Attachment(s) Alert & Compare Category...	Attachment(s) Modified
<input type="checkbox"/>	Default document open location	<input type="text"/>
<input type="checkbox"/>	Default email attachment format	Portable Document Format (.pdf) ▼
<input type="checkbox"/>	Default Redline save location	<input type="text"/>
<input type="checkbox"/>	Default rendering set	<input type="text"/>
<input checked="" type="checkbox"/>	Display document description as well as document ID	
<input checked="" type="checkbox"/>	Display Document Selection dialog on startup	
<input checked="" type="checkbox"/>	Display Redline in page layout view	
<input type="checkbox"/>	Display source document labels	
<input type="checkbox"/>	Display source documents in page layout view	
<input type="checkbox"/>	Display table gridlines	

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.



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 and PowerPoint 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:

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

### Microsoft Word Documents

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOCM Format	DOC Format	DOCX/DOCM Format
<b>Track Changes</b>	√ Deleted	√ Deleted	√ Deleted, but where track change deletes text, the text is turned into hidden spaces (revealed if turn on "show hidden text")	√ Deleted
<b>Comments</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>Small Text</b>	√ Deleted	√ Deleted	√ Deleted, but turned into hidden spaces (revealed if turn on "show hidden text")	√ Deleted
<b>Color on Color Text (includes White Text)</b>	√ 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
<b>Hidden Text</b>	√ Deleted	√ Deleted	√ Deleted, but turned into hidden spaces (revealed if turn on "show hidden text")	√ Deleted
<b>Versions</b>	√ Deleted	<b>NA</b>	√ Deleted	<b>NA</b>
<b>Authors</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>AutoVersion</b>	√ Cleared	<b>NA</b>	√ Cleared	<b>NA</b>
<b>Custom Properties (found in the Custom tab)</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>Document Variables</b>	√ Deleted	<b>X</b>	√ Name and value turned into spaces but the document variable still exists	√ Deleted
<b>Macros</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>Routing Slip</b>	√ Deleted	<b>NA</b>	√ Deleted	<b>NA</b>
<b>Reviewers</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>Footnotes</b>	√ Deleted	√ Deleted	√ 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
<b>Fields</b>	√ 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
<b>Hyperlinks</b>	√ 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
<b>Document Statistics (found in the Statistics tab)</b>	√ Deleted	X	√ Deleted "Last Saved By" and other fields reset.	√ Deleted "Last Saved By" and other fields reset.
<b>Built-In Properties – Standard Properties (found in the Summary and Contents tabs)</b>	√ Deleted	√ Deleted	√ Deleted "Title"	√ Deleted
<b>Smart Tags</b>	√ Deleted	√ Deleted	√ Deleted	√ Deleted
<b>Template</b>	√ 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"
<b>Headers</b>	X	√ Checks headers in same way as body text	X	√ Checks headers in same way as body text
<b>Footers</b>	X	√ Checks footers in same way as body text	X	√ Checks footers in same way as body text

Feature	Clean		Lightspeed Clean	
	DOC Format	DOCX/DOC M Format	DOC Format	DOCX/DOC M Format
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
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	√	√	√	√
Small Text	X	√	X	√
Color on Color Text (includes White Text)	X	√	X	√
Authors	√	√	√	√
Custom Properties (found in the Custom tab)	√	√	√	√
Macros	X	X	√	√
Routing Slip	√	NA	√	NA
Hyperlinks	X	X	√	√
Document Statistics (found in the Statistics tab)	√	X	√	√

Feature	Clean		Lightspeed Clean	
	XLS Format	XLSX/XLSM Format	XLS Format	XLSX/XLSM Format
<b>Built-In Properties – Standard Properties (found in the Summary and Contents tabs)</b>	√	√	√	√
<b>Smart Tags</b>	X	X	X	X
<b>Headers</b>	√	√	√	√
<b>Footers</b>	√	√	√	√
<b>Text Within Text Box</b>	X	X	X	X
<b>SmartArt</b>	NA	X	NA	X

## Microsoft PowerPoint Presentations

Feature	Clean		Lightspeed Clean	
	PPT Format	PPTX/PPTM Format	PPT Format	PPTX/PPTM Format
<b>Comments</b>	√	√	√	√
<b>Small Text</b>	X	X	X	X
<b>Color on Color Text (includes White Text)</b>	X	X	X	X
<b>Authors</b>	√	√	√	√
<b>Custom Properties (in the Custom tab)</b>	√	√	√	√
<b>Macros</b>	X	X	√	√
<b>Hyperlinks</b>	X	X	√	√
<b>Document Statistics (in the Statistics tab)</b>	X	√	√	X

Feature	Clean		Lightspeed Clean	
	PPT Format	PPTX/PPTM Format	PPT Format	PPTX/PPTM Format
<b>Built-In Properties – Standard Properties (in the Summary and Contents tabs)</b>	√	√	√	√
<b>Smart Tags</b>	X	X	X	X
<b>Template</b>	X	X	X	X
<b>Headers</b>	X	X	X	√
<b>Footers</b>	X	X	X	√
<b>Text Within Text Box</b>	X	X	X	X
<b>SmartArt</b>	NA	X	NA	X
<b>Speaker Notes</b>	√	√	√	√
<b>Hidden Slides</b>	√	√	√	√