Workshare Protect 10.4

User Guide

Table of Contents

Chapter 1: Introducing Workshare Protect

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

- **What is Workshare Protect?**, page 5, introduces Workshare Protect.
- **Workshare Protect Functionality**, page 5, describes the different areas of functionality of Protect.
- **Accessing Protect Functionality**, page 7, describes how to access Protect functionality after install.
- **Licensing**, page 9, describes how to license Protect after install.

What is Workshare Protect?

Workshare Protect helps companies eliminate the risk of accidentally sharing sensitive data, without interrupting established workflows.

Key features of Workshare Protect include:

- Advanced, interactive metadata cleaning and PDF creation for attachments in Outlook and open documents
- Comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well as visible sensitive data
- Centralized policy design and enforcement administrator tools

***Note**: Workshare Protect can be installed without Microsoft Office integration. In this case, the metadata removal functionality is only available when sending emails.*

Workshare Protect Functionality

Workshare Protect provides sophisticated functionality that is convenient and accessible, enabling users to move smoothly between tasks and work rapidly to manage changes. Workshare Protect assists you throughout the complete document lifecycle – from document assembly, review, verification and security.

File and metadata security

Workshare Protect provides content risk protection through comprehensive cleaning of metadata and conversion to secure PDF.

Protect enables the discovery and removal of hidden sensitive data as well visible sensitive data. Hidden sensitive data may include information such as track changes, author’s name, server names, keywords, routing slips and authoring trails.

On your desktop

Protect integrates with 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). After discovery, users can remove selected metadata.

Protect quickly and securely converts Office documents into PDF or PDF/A files. Users can access PDF conversion functionality from within Word, Excel and PowerPoint or by right-clicking closed Office files from the desktop and from within a DMS/CRM or SharePoint. Additionally users 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.

Within email

Protect can be configured to support the way you work.

Interactive Protect offers options to control documents and secure attachments before sending email. It simplifies metadata cleaning, avoids email pop-ups, and eliminates Outlook add-in issues. Protect scans documents as soon as they are added as attachments to an email. Users are made aware of the risk involved and given the option to make informed decisions before clicking Send. From the Interactive Protect panel users can clean metadata from attachments, convert attachments to PDF or PDF/A, and compress attachments into one zip file.

In other configurations, 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 user details to be included in documents sent externally, but it may be fine to leave those details in documents sent within an organization. Protect comes with a pre-defined default security profile (collection of policies).

DMS/CRM integration

Workshare Protect can integrate with your DMS or CRM as well as SharePoint to provide PDF functionality.

***Note**: To integrate with a DMS/CRM or SharePoint, Workshare Protect must be installed with the relevant integration selected and additional details may need to be configured in the Workshare Configuration Manager. Refer to your system administrator for further information.*

The specific functionality available with each DMS/CRM integration is detailed in the table below:

Functionality	iManage	Net Documents	OpenText	Worldox	SharePoint
From within DMS, Convert to PDF with Workshare	✓	✓	✓	✓	✗
From within DMS, Combine files in Workshare	✓	✗	✓	✓	✗

***Note**: The right-click options are not currently available in iManage Work 10.*

Accessing Workshare Protect

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

After you have installed Protect, the Litera tab is added to the ribbon in your Microsoft Office applications - Word, Excel and PowerPoint. The addition of Protect does not affect the standard functionality of Word, Excel or PowerPoint. You can operate these applications as usual and access the Protect functionality as required.

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

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

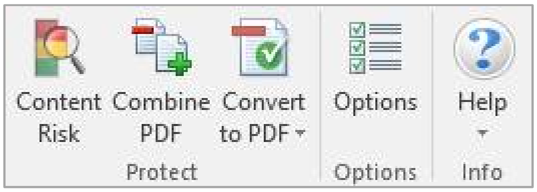
***Note**: Workshare Protect can be installed without Microsoft Office integration. In this case, the Litera tab is not available. The Workshare metadata removal functionality is only available when sending emails.*

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 Office documents at the same time. Refer to Batch cleaning, for further information.

Workshare toolbar options

In Office applications, the Workshare toolbar options are included in the Litera tab as follows:



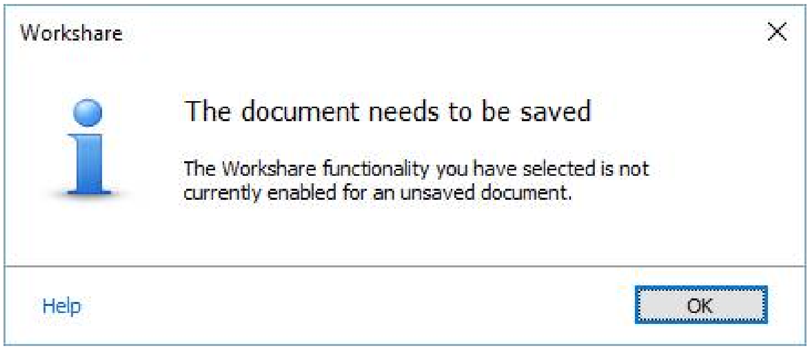
Whether these options are included in the ribbon is configurable from the **General > User Interface** category in the Workshare Configuration Manager. Refer to *Workshare Configuration Options* for further information*.*

The Workshare toolbar options are as follows:

Group	Item	Description
Protect	**Content Risk**	Enables you to display a report of all the content risk in a document as well as remove selected hidden data from the document. Refer to *Displaying Content Risk in Documents* for further information.
	Combine PDF	Enables you to combine multiple files into a single PDF file. Refer to *PDF Combine* for further information.
	Convert to PDF	Enables you to convert documents to PDF. Refer to *Cleaning options* for further information.
Options	**Options**	Enables you to configure system parameters in the Workshare Configuration Manager. Refer to *Introducing the Workshare Configuration Manager* for further information.
Info	**Help**	Provides access to version, copyright and license information about Workshare Protect as well as online help.

Enabling Workshare Protect functionality

To ensure Workshare Protect functionality is *fully* enabled, you should work with saved documents. If you are working in Microsoft Office on an unsaved document and you select **Combine PDF**, the following message is displayed:



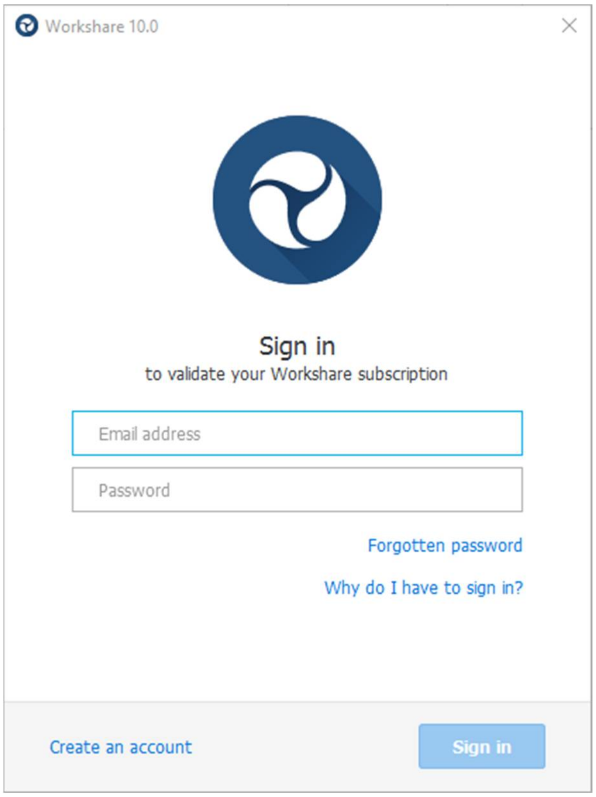
Workshare

The document needs to be saved

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

Licensing

After installation, you are prompted to log in to your Workshare account in order to retrieve your license entitlements. This prompt displays the first time you access Workshare functionality, for example, by clicking any Workshare option in the ribbon. You will see the following:



Workshare 10.0

Sign in

to validate your Workshare subscription

***Note**: You can also open the Workshare Configuration Manager, select the **My Products** tab and click **Sign in**.*

Enter your Workshare credentials (email address and password) for Workshare and click **Sign in**. Your license entitlements are retrieved and you have access to all Workshare functionality. Your license entitlements are shown in the **My Products** tab of the Workshare Configuration Manager.

Users who do not yet have a Workshare account can click **Create an account** in the login dialog. Workshare checks their email address and will automatically register them against your corporate Workshare account and update their license entitlement.

Chapter 2: Protecting 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 – Protection on your Desktop**, page 12, introduces the ways in which Workshare Protect enables you to protect documents by viewing and removing sensitive content risk.
- **Displaying Content Risk in Documents**, page 12, describes how to discover all content risk in Office documents.
- **Cleaning Hidden Data**, page 14, describes how to remove selected types of hidden data from a document and from multiple documents.
- **Converting to PDF**, page 20, describes how to secure your documents by converting to PDF.

Overview – Protection on your Desktop

***Note:** This chapter describes how to protect documents on your desktop by removing metadata and converting to PDF. The protection of documents when emailing is described in Chapter 3: Protecting Attachments.*

Workshare Protect offers complete protection of files to ensure they are fully secure before distribution. Discover what hidden metadata remains in your document, clean it and then convert the document to PDF ensuring a safe and secure file.

Protect provides comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well visible sensitive data. Hidden sensitive data may include information such as track changes, author's name, server names, keywords, routing slips and authoring trails. Protect integrates with Office providing an option to display a comprehensive report of all the content risk in a document, displayed according to its risk level (high, medium, low).

Workshare Protect creates the most secure PDF files available from any application. You can quickly and easily convert open and closed Microsoft Office documents into PDF or PDF/A removing hidden data from the document and setting security options as you do so. Workshare Protect also provides "PDF Anywhere" which is the ability to convert a document to PDF from any application.

***Note**: PDF creation can also be enforced on email attachments leaving your organization. Refer to Chapter 3: Protecting Attachments.*

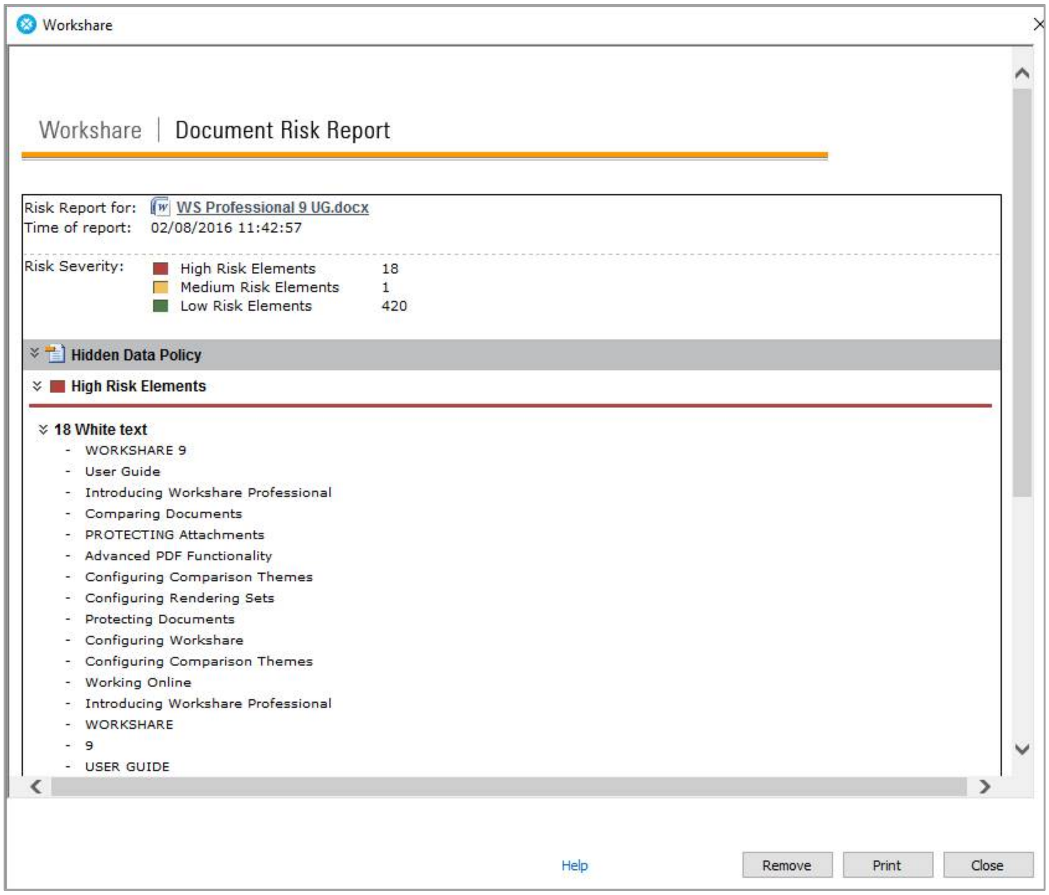
Displaying Content Risk in Documents

Workshare Protect integrates with Microsoft Office to provide an option to discover and view content risk in Microsoft Word, Excel or PowerPoint documents.

To discover content risk in your document:

1. Open your document and click **Content Risk**, (**Protect** group) in the Litera tab.

   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 a summary of the content risk found.

   Risk Report for: WS Professional 9 UG.docx
   Time of report: 02/08/2016 11:42:57

Risk Severity:		
🟥	High Risk Elements	18
🟨	Medium Risk Elements	1
🟩	Low Risk Elements	420

   Hidden Data Policy

   🟥 High Risk Elements

   18 White text
   - WORKSHARE 9
   - User Guide
   - Introducing Workshare Professional
   - Comparing Documents
   - PROTECTING Attachments
   - Advanced PDF Functionality
   - Configuring Comparison Themes
   - Configuring Rendering Sets
   - Protecting Documents
   - Configuring Workshare
   - Configuring Comparison Themes
   - Working Online
   - Introducing Workshare Professional
   - WORKSHARE
   - 9
   - USER GUIDE

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

2. To display details of the content risk found, click ︽ to the left of the content risk type.

3. To remove hidden data from the document, use the **Remove** button. Refer to *Cleaning Hidden Data*, for more details.

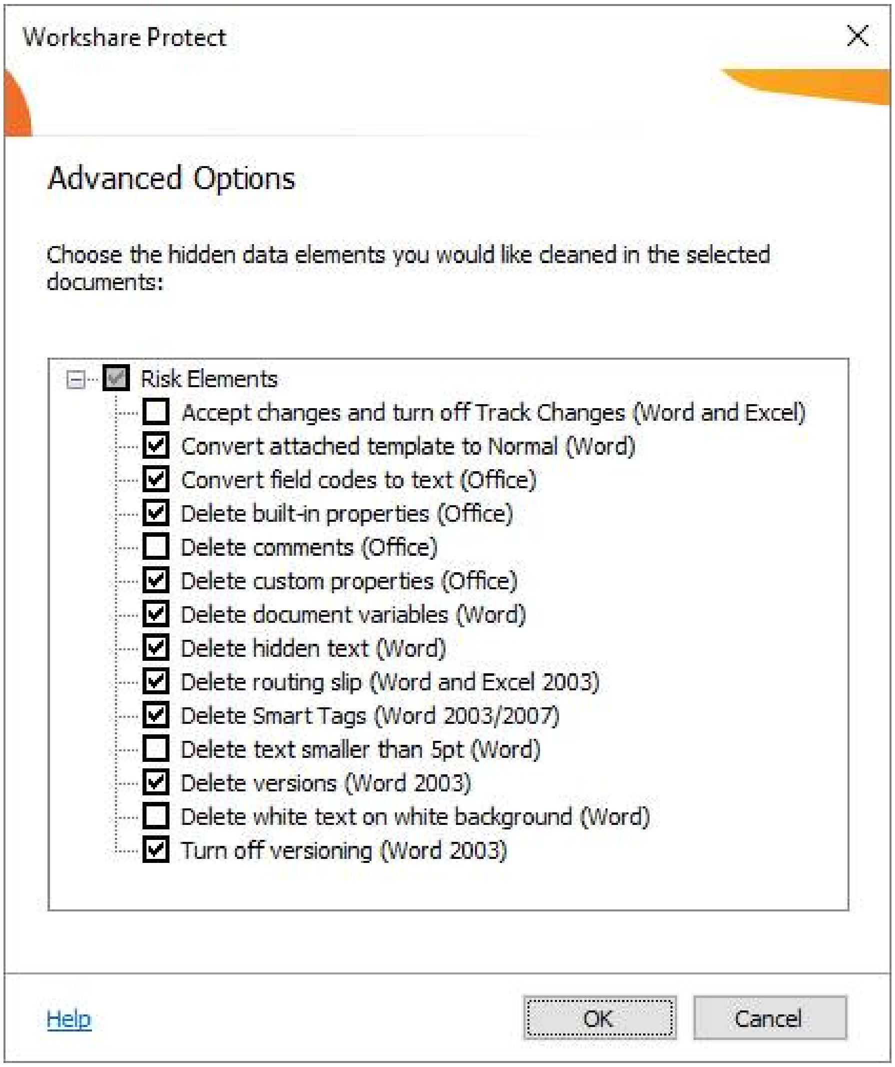
4. To print the report, click **Print**.

Cleaning Hidden Data

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

To remove hidden data:

1. Click **Remove** in the Document Risk Report. The *Advanced Options* dialog is displayed.



Workshare Protect

Advanced Options

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

- ☑ Risk Elements
  - □ Accept changes and turn off Track Changes (Word and Excel)
  - ☑ Convert attached template to Normal (Word)
  - ☑ Convert field codes to text (Office)
  - ☑ Delete built-in properties (Office)
  - □ Delete comments (Office)
  - ☑ Delete custom properties (Office)
  - ☑ Delete document variables (Word)
  - ☑ Delete hidden text (Word)
  - ☑ Delete routing slip (Word and Excel 2003)
  - ☑ Delete Smart Tags (Word 2003/2007)
  - □ Delete text smaller than 5pt (Word)
  - ☑ Delete versions (Word 2003)
  - □ Delete white text on white background (Word)
  - ☑ Turn off versioning (Word 2003)

A complete list of hidden data that can be removed, reset or converted is listed in the dialog. Different options will appear according to the type of document – Word, Excel or PowerPoint. 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 options.
3. After making your selection, click **OK**. The selected hidden data is removed from the document.

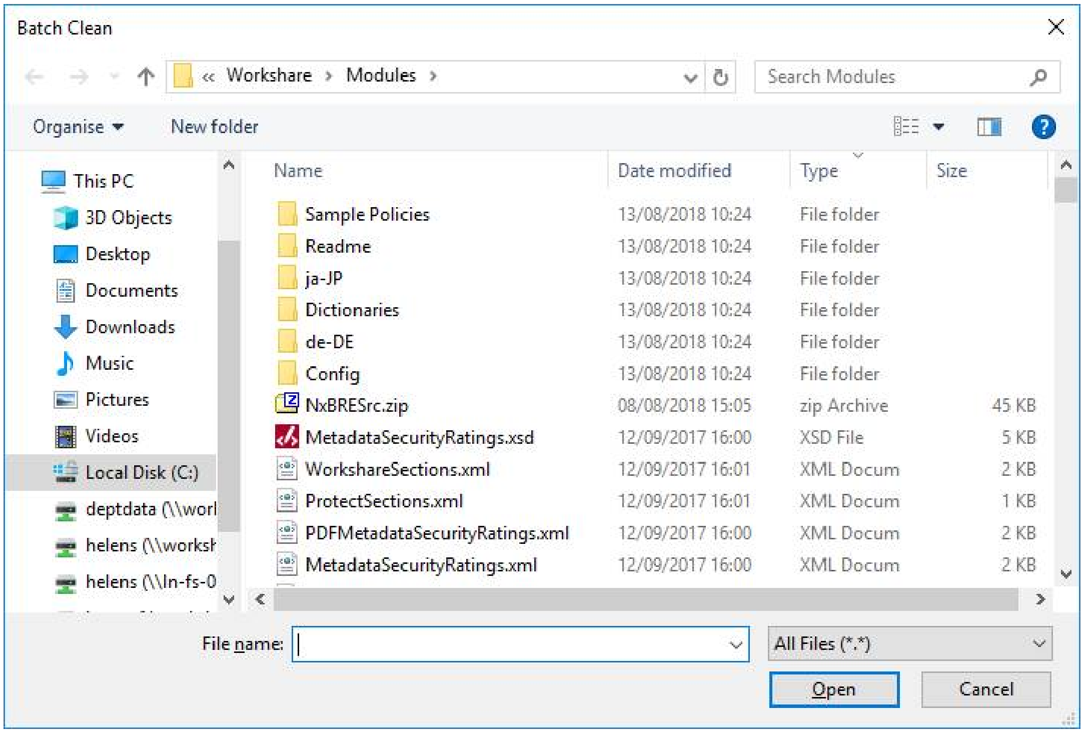
Workshare Protect may take a few moments to clean you document depending on the size of the document and the amount of hidden data to be removed. The Document Risk Report is updated after the document has been cleaned to show any remaining content risk. After cleaning, the document with hidden data removed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

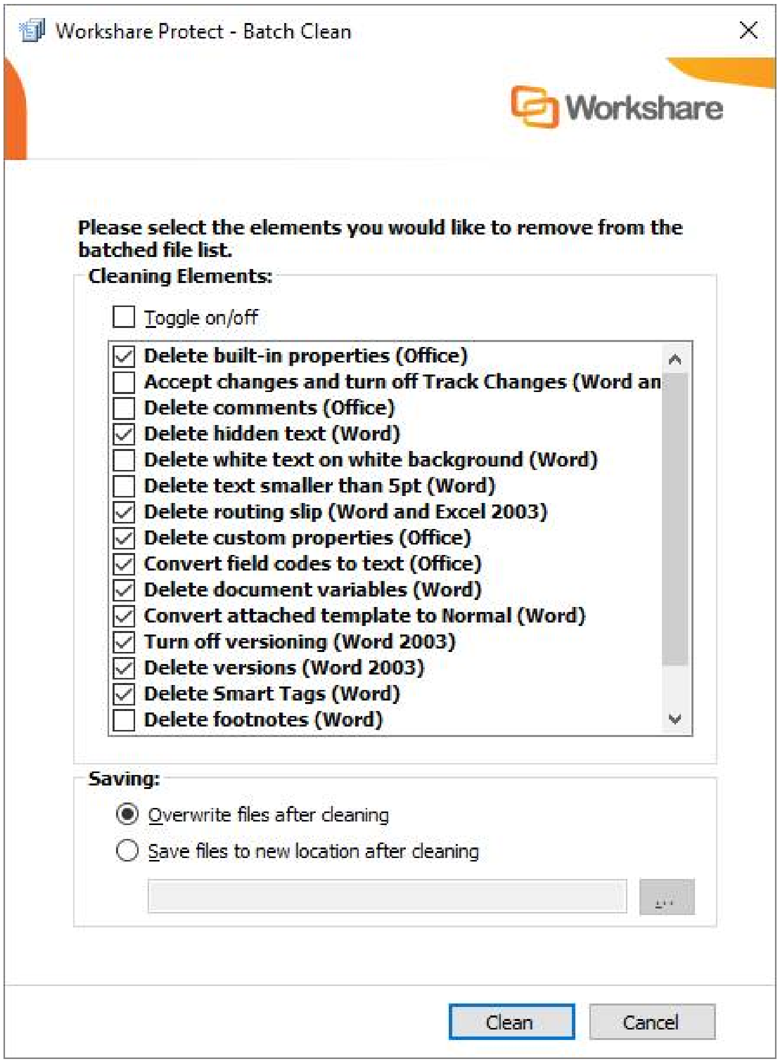


Name	Date modified	Type	Size
Sample Policies	13/08/2018 10:24	File folder	
Readme	13/08/2018 10:24	File folder	
ja-JP	13/08/2018 10:24	File folder	
Dictionaries	13/08/2018 10:24	File folder	
de-DE	13/08/2018 10:24	File folder	
Config	13/08/2018 10:24	File folder	
NxBRESrc.zip	08/08/2018 15:05	zip Archive	45 KB
MetadataSecurityRatings.xsd	12/09/2017 16:00	XSD File	5 KB
WorkshareSections.xml	12/09/2017 16:01	XML Docum	2 KB
ProtectSections.xml	12/09/2017 16:01	XML Docum	1 KB
PDFMetadataSecurityRatings.xml	12/09/2017 16:00	XML Docum	2 KB
MetadataSecurityRatings.xml	12/09/2017 16:00	XML Docum	2 KB

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

2. Select the documents you want to clean. Press the **Ctrl** or 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 File Explorer, then right-click and select **Send To** then **Batch Clean**.*



Workshare Protect - Batch Clean

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

Cleaning Elements:

□ Toggle on/off

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

Saving:

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

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

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

> ***Note**: The metadata that is selected to be removed by default is according to the Content Risk settings in the Workshare Configuration Manager (**Protection > Remove Metadata** category).*

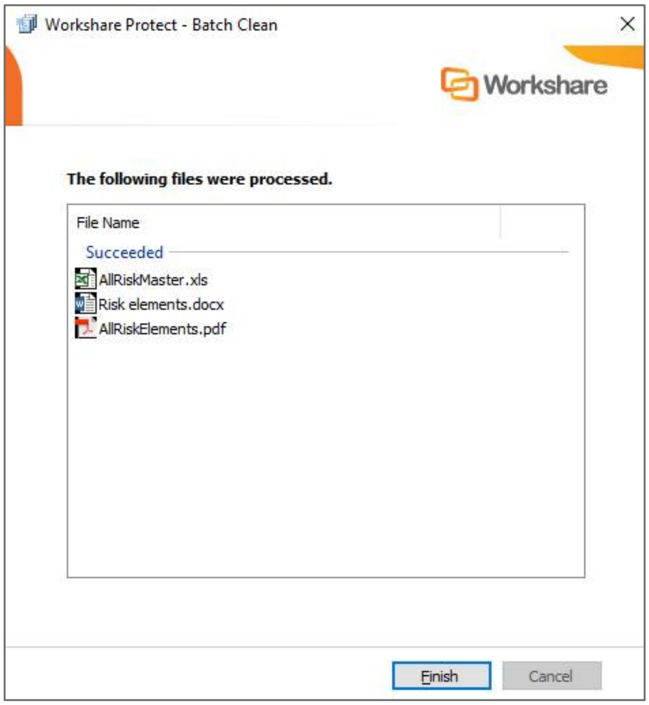
> ***Tip!** Select the **Toggle on/off** checkbox to select/deselect all the hidden data options.*

5. Select one of the following save options:
   - **Overwrite files after cleaning**: Selecting this option will save the cleaned files over the original files, overwriting the existing version.

> ***Note**: You must have 'write' permissions on the file in order to overwrite the original. If you do not have 'write' permissions on all files selected, this option is disabled.*

   - **Save files to new location after cleaning**: Selecting this option will save the cleaned files to a different location, leaving the original files in their original location and in an uncleaned state. Click the browse button and select the new save location.

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



The following files were processed.

File Name

Succeeded

AllRiskMaster.xls
Risk elements.docx
AllRiskElements.pdf

7. Click **Finish**.

Batch cleaning using a command line

Batch cleaning can be performed using the command line.

To batch clean using the command line:

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

- To clean hidden data from the entire hard disk:

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

- To clean all hidden data from a single document:

  ```
  bc-console.exe "<filepath>" /all
  ```

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

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

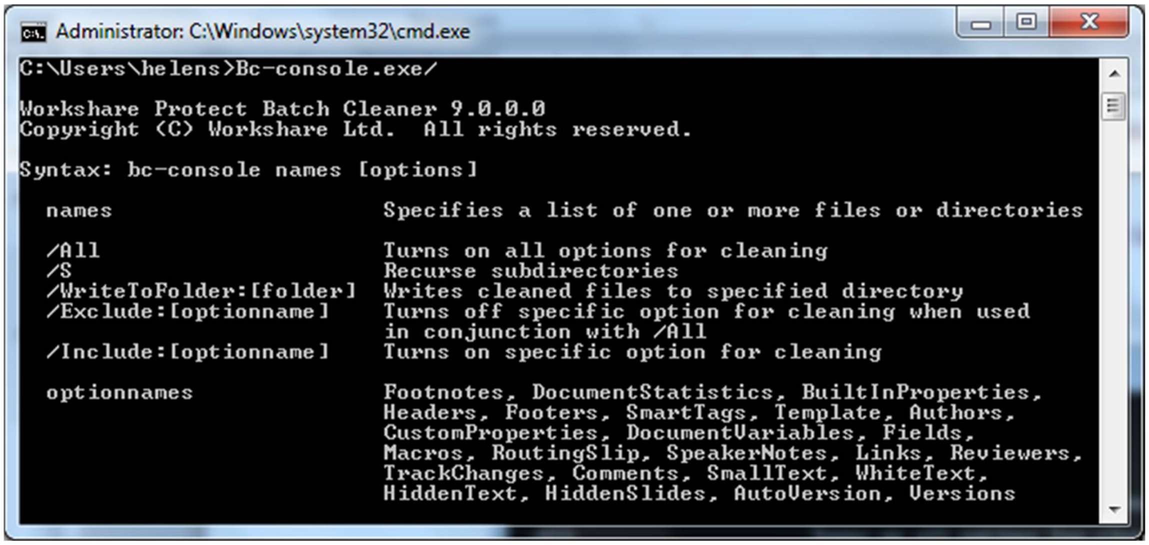
  ```
  Bc-console.exe "<filepath>" /all /exclude:comments
  /exclude:trackchanges
  ```

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

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

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

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



```
C:\Users\helens>Bc-console.exe/

Workshare Protect Batch Cleaner 9.0.0.0
Copyright (C) Workshare Ltd.  All rights reserved.

Syntax: bc-console names [options]

  names                     Specifies a list of one or more files or directories

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

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

The options are described in the following table:

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

Cleaning options

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

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

Option	Description
Delete built-in properties (Office)	Microsoft Word, Excel and PowerPoint. Removes all summary properties - author, category, comments, company, keywords, manager, title, subject, and hyperlink base; and custom properties – text, date and number.
Delete comments (Office)	Microsoft Word, Excel and PowerPoint. Removes any comments embedded in the document.
Delete custom properties (Office)	Microsoft Word, Excel and PowerPoint. Removes any custom properties that have been added to the document.
Delete document variables (Word)	Microsoft Word only. Deletes all document variables. Document variables are values stored in Microsoft Word documents that are used by either field codes or macros. These variables may contain confidential information like company names or file locations. Even if field codes and macros are removed, the variables used may remain in the document. Variables can be viewed in Microsoft Word in the Visual Basic Editor.
Delete footers (Excel and PowerPoint)	Microsoft Excel and PowerPoint. Removes any footers included in the sheet or slide.
Delete headers (Excel and PowerPoint)	Microsoft Excel and PowerPoint. Removes any headers included in the sheet or slide. ***Note**: Headers and footers cannot be removed from PowerPoint documents when using Lightspeed clean.*
Delete hidden slides (PowerPoint)	Microsoft PowerPoint only. Removes hidden slides from Microsoft PowerPoint files. Hidden slides are not required for a slide show (they are not automatically displayed during a slide show) but they may contain confidential information.
Delete hidden text (Word)	Microsoft Word only. Removes all text that has been formatted as hidden.
Delete links (Excel)	Microsoft Excel only. Converts external links in Microsoft Excel files to text. The following are examples of external links: • Link to a cell in another Microsoft Excel document. • Named link to a named reference in another Microsoft Excel document. • Link to another document. • OLE link that inserts another document as an icon. • OLE link that inserts another document as text.

Option	Description
Delete macros (Word and Excel)	Microsoft Word and Excel. Removes VBA macros from a document. This feature is not intended as virus protection, but rather to protect any confidential information, intellectual property or formulas included in the macros.
Delete markups (PDF)	PDF only. Removes any markup in a PDF file. Markup is a tool used to make comments and annotations to PDF documents.
Delete properties (PDF)	PDF only. Removes properties in a PDF file. Standard properties are details about a file that help identify it, including its title, subject, author, manager, company, category, keywords, comments, and hyperlink base. ***Note**: Removing properties from a PDF/A file will disable its PDF/A status.*
Delete routing slip (Word and Excel 2003)	Microsoft Word and Excel. Removes all entries from a routing slip, as well as the message subject and text. This can prevent email addresses of colleagues from being unknowingly distributed. This also deletes any envelope information, such as recipients, subject, and introduction, which are used when sending to a mail recipient.
Delete Smart Tags (Word 2003/2007)	Microsoft Word only. Removes smart tags from Microsoft Word documents. Smart tags are added to your documents as you create them if the option is enabled. These tags are linked to particular text in a document, such as a name, and allow you to perform certain actions by selecting the link associated with the text. Depending on the smart tag functions you use, they may embed extra hidden information in your document. Smart tags only exist in Microsoft Office XP to 2010.
Delete Speaker Notes (PowerPoint)	Microsoft PowerPoint only. Deletes all text that appears on the Notes Page in a Microsoft PowerPoint presentation. This is usually used by speakers to remind them of points during a presentation. You may want to remove speaker notes before distributing a presentation, as they are not usually intended for others to read.
Delete text smaller than 5pt (Word)	Microsoft Word only. Removes all text that has been formatted with a font size less that 5pt (i.e. 4pt and less). Small text can also be detected in Microsoft Excel but it is not cleaned.
Delete versions (Word 2003)	Microsoft Word only. Removes any previous versions of the document that you may have saved. Previous versions can be useful while you are developing a document, but often they can contain confidential information that you have removed from the main document.

Option	Description
Delete white text on white background (Word)	Microsoft Word only. Removes all text with a white font that has been formatted with a white background color.
Turn off versioning (Word 2003)	Microsoft Word only. Turns off the flag to automatically save a new version of the document every time the document is closed. This applies to local file systems only. Versions can still be saved manually by saving a file with a different name.

Converting to PDF

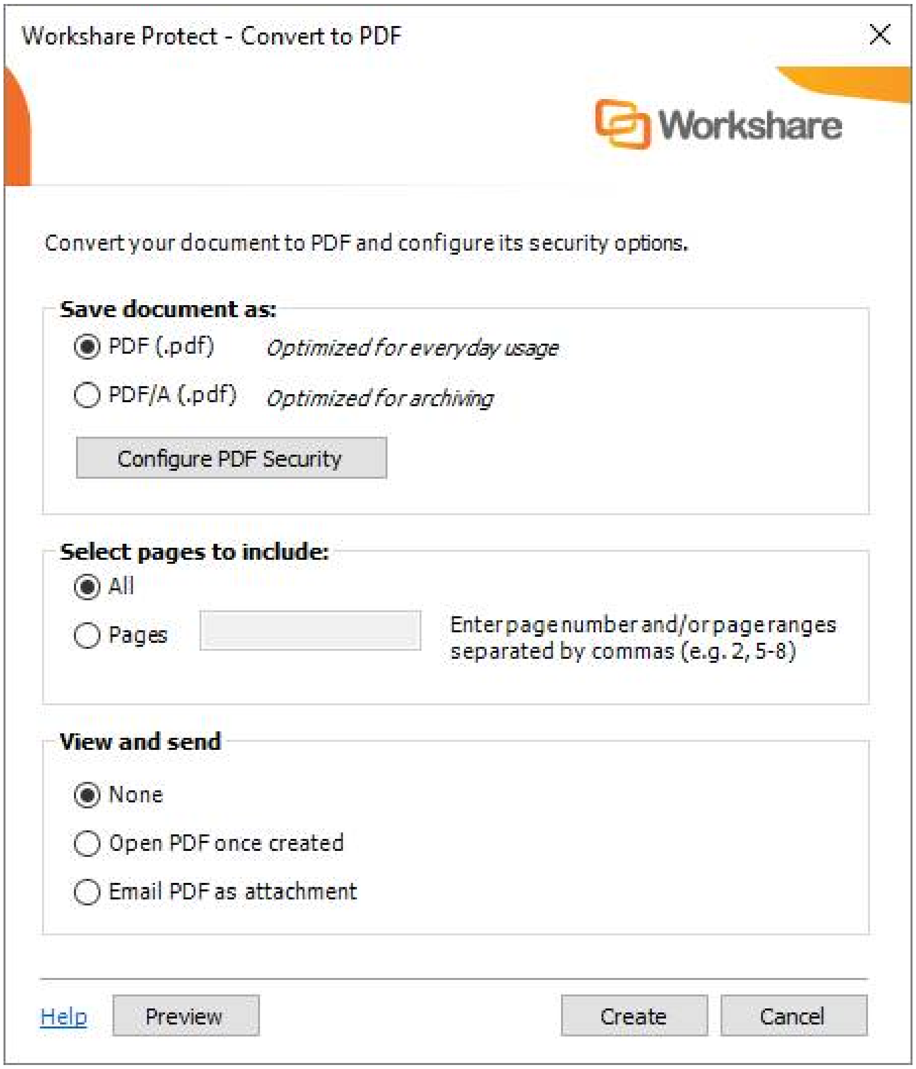
At any time when working on a document in Microsoft Word, Excel or PowerPoint, you can convert the document into PDF or PDF/A. This is useful if you want to maintain a file in its current format, as PDF documents cannot be edited as easily as Microsoft Word, Excel and PowerPoint documents. This functionality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

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

To convert a document to PDF or PDF/A:

1. Start in either of the following ways:
   - With your document open in Microsoft Word, Excel or PowerPoint, click **Convert to PDF** (**Protect** group) in the Litera tab.
   - Right-click a 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.



Workshare Protect - Convert to PDF

Convert your document to PDF and configure its security options.

Save document as:

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

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

Select pages to include:

● All

○ Pages

Enter page number and/or page ranges separated by commas (e.g. 2, 5-8)

View and send

● None

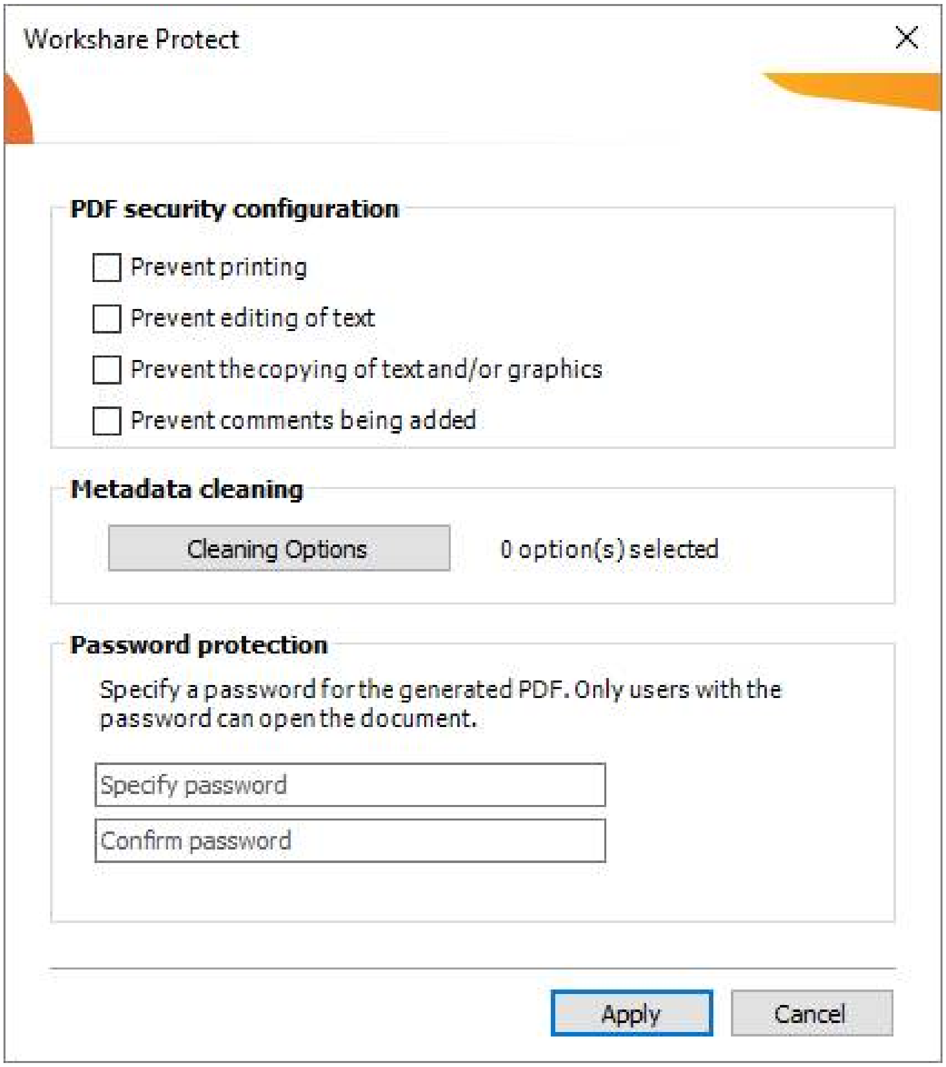
○ Open PDF once created

○ Email PDF as attachment

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

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

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



Workshare Protect

PDF security configuration

☐ Prevent printing

☐ Prevent editing of text

☐ Prevent the copying of text and/or graphics

☐ Prevent comments being added

Metadata cleaning

Cleaning Options   0 option(s) selected

Password protection

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

Specify password

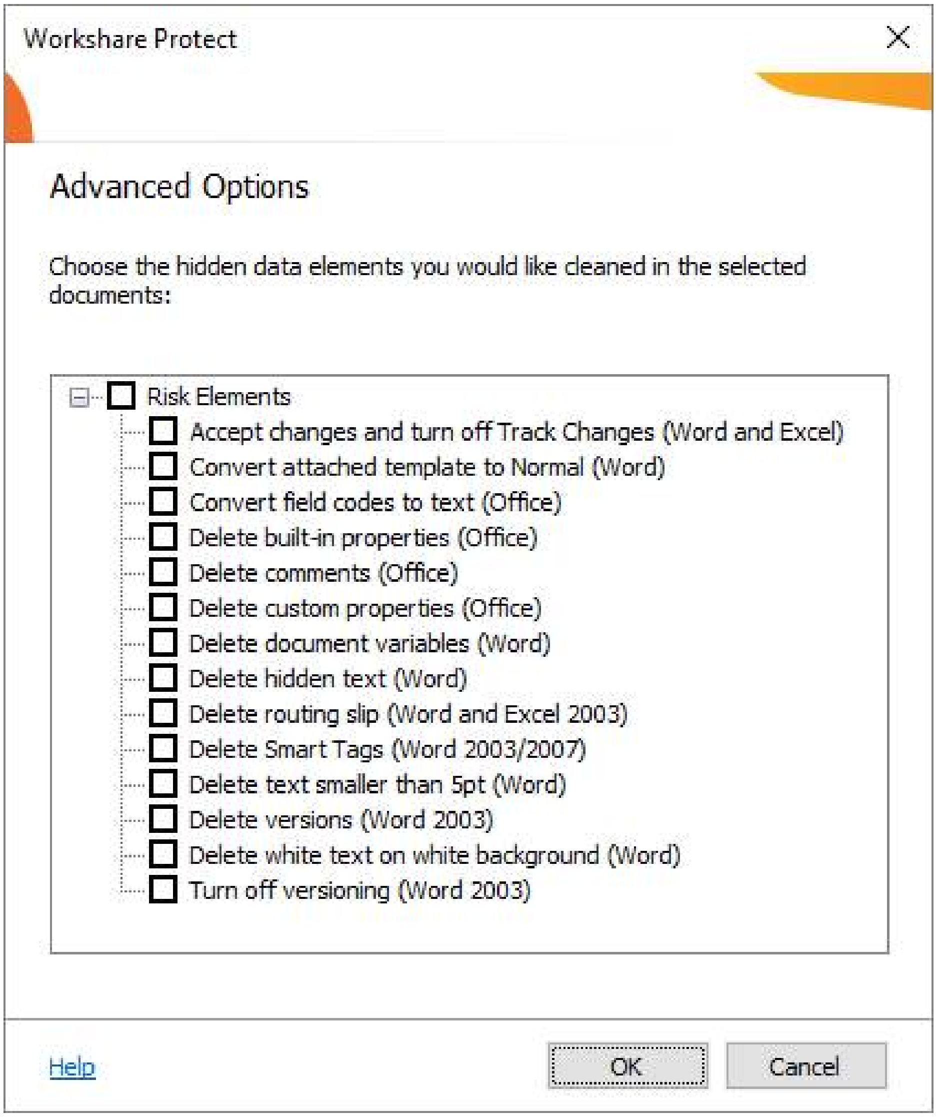
Confirm password

Apply   Cancel

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

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

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



Workshare Protect

Advanced Options

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

- □ Risk Elements
  - □ Accept changes and turn off Track Changes (Word and Excel)
  - □ Convert attached template to Normal (Word)
  - □ Convert field codes to text (Office)
  - □ Delete built-in properties (Office)
  - □ Delete comments (Office)
  - □ Delete custom properties (Office)
  - □ Delete document variables (Word)
  - □ Delete hidden text (Word)
  - □ Delete routing slip (Word and Excel 2003)
  - □ Delete Smart Tags (Word 2003/2007)
  - □ Delete text smaller than 5pt (Word)
  - □ Delete versions (Word 2003)
  - □ Delete white text on white background (Word)
  - □ Turn off versioning (Word 2003)

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

7. Click **OK**.

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

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

9. Click **Apply**.

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

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

11. In the **View and send** area, select the **Open PDF once created** checkbox if you want the PDF to be opened once it has been created or select the **Email PDF as attachment** checkbox if you want the PDF to be attached to an email once it has been created.
12. If required, click **Preview** to view the document as a PDF.
13. Click **Create**.
14. In the Save dialog, specify the name and location for the PDF file and click **Save**. The document is converted to PDF or PDF/A. If you selected **Open PDF once created**, the new PDF is opened. If you selected **Email PDF as attachment**, an email message window is displayed with the PDF as an attachment.

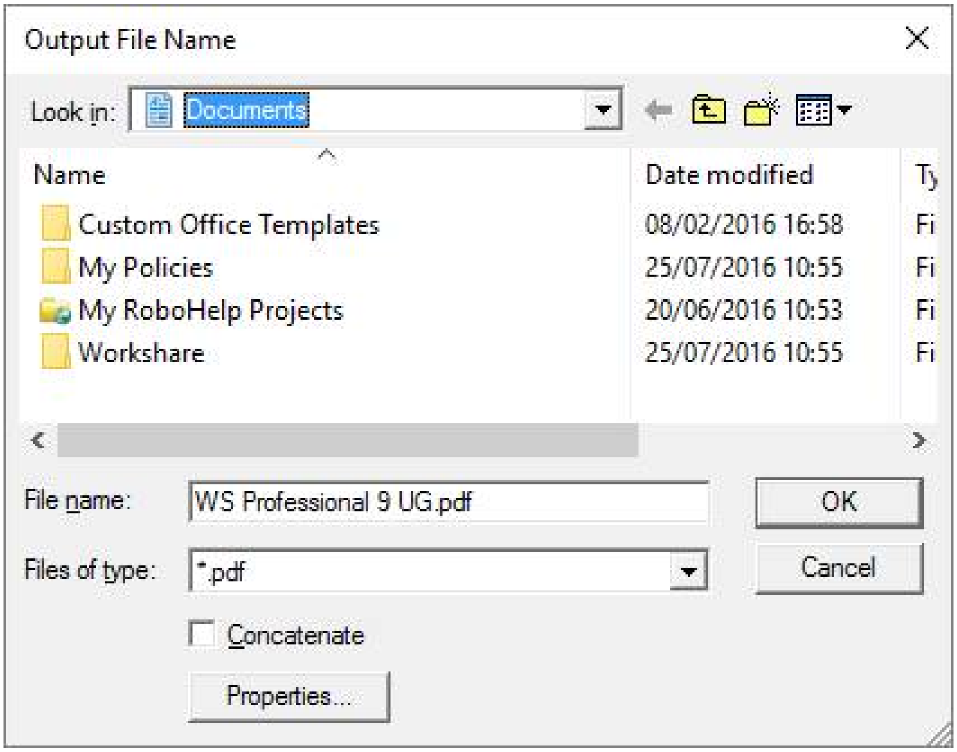
PDF anywhere

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

To convert to PDF from anywhere:

1. Click **Print** in the application.
2. Select **Workshare PDF Publisher** as the printer.

3. Specify other settings as required and click **Print**. The *Output File Name* dialog is displayed.



Look in: Documents

Name	Date modified	Ty
Custom Office Templates	08/02/2016 16:58	Fi
My Policies	25/07/2016 10:55	Fi
My RoboHelp Projects	20/06/2016 10:53	Fi
Workshare	25/07/2016 10:55	Fi

File name: WS Professional 9 UG.pdf

Files of type: *.pdf

□ Concatenate

4. Specify a name for the PDF in the **File name** field or, if you want to add to an existing PDF, select the **Concatenate** checkbox and browse to and select the existing PDF.

5. Click **OK**. The open document is converted to PDF and saved as specified or added to an existing PDF.

Chapter 3: Protecting Attachments

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

- **Introducing Attachment Protection**, page 30, introduces how Workshare Protect protects your files when sending by email.
- **Interactive Protect**, page 33, describes how to use Interactive Protect to secure your emails.
- **Using the Protect Profile Dialog**, page 41, describes how to send secure emails using the Workshare Protect Profile dialog.
- **Using the Email Security Dialog**, page 43, describes how to send secure emails using the Workshare Protect Email Security dialog.

Introducing Attachment Protection

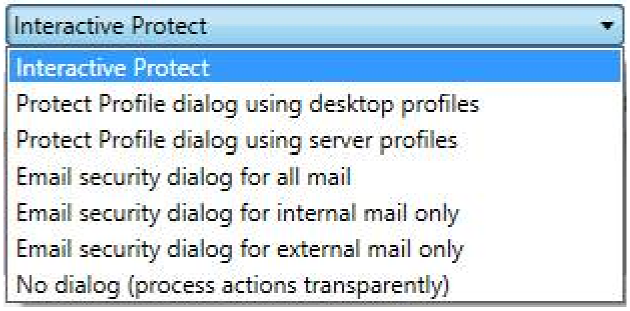
***Note:** This chapter describes how to protect documents when emailing by removing metadata or converting to PDF. The protection of documents on your desktop is described in Chapter 2: Protecting Documents.*

Workshare Protect provides security and protection for email attachments. It is able to process the emails you send to ensure security in the following ways:

- Remove metadata from attachments
- Convert attachments to PDF or PDF/A
- Compress multiple attachments into a single zip file

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

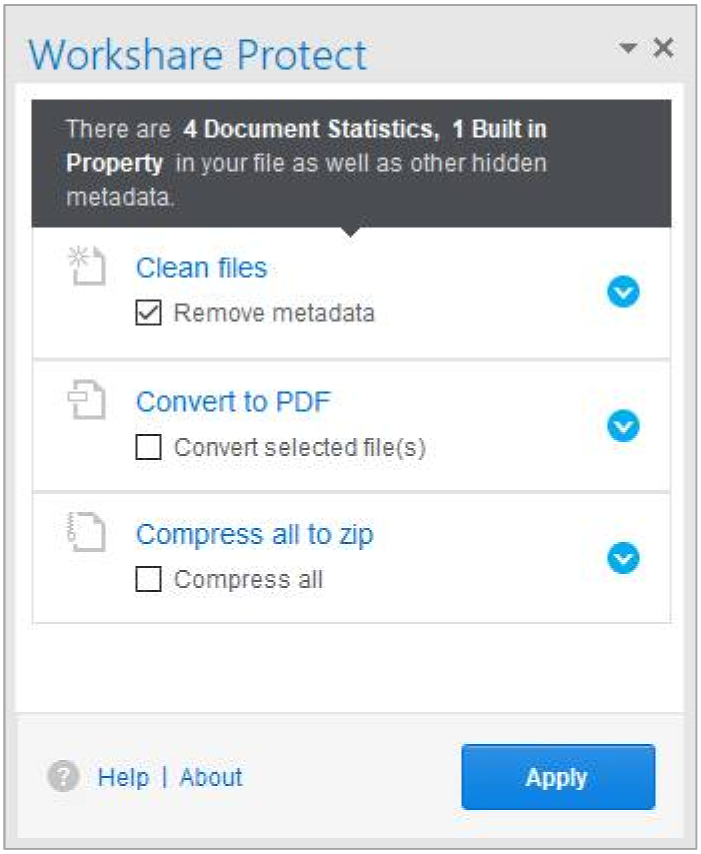
When Workshare Protect is “on”, the user experience when sending emails will vary depending on which option your administrator has selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).


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

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

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

Interactive Protect panel



Workshare Protect

There are **4 Document Statistics, 1 Built in Property** in your file as well as other hidden metadata.

Clean files

☑ Remove metadata

Convert to PDF

□ Convert selected file(s)

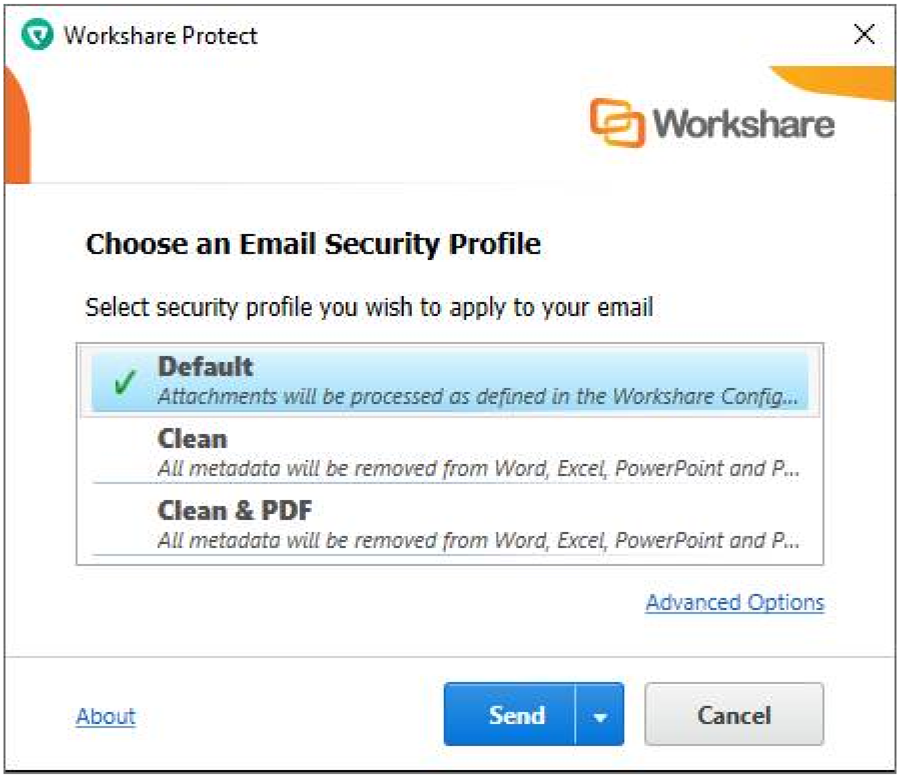
Compress all to zip

□ Compress all

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

The Interactive Protect panel is described in *Using Interactive Protect*.

Protect Profile dialog



Workshare Protect

Choose an Email Security Profile

Select security profile you wish to apply to your email

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

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

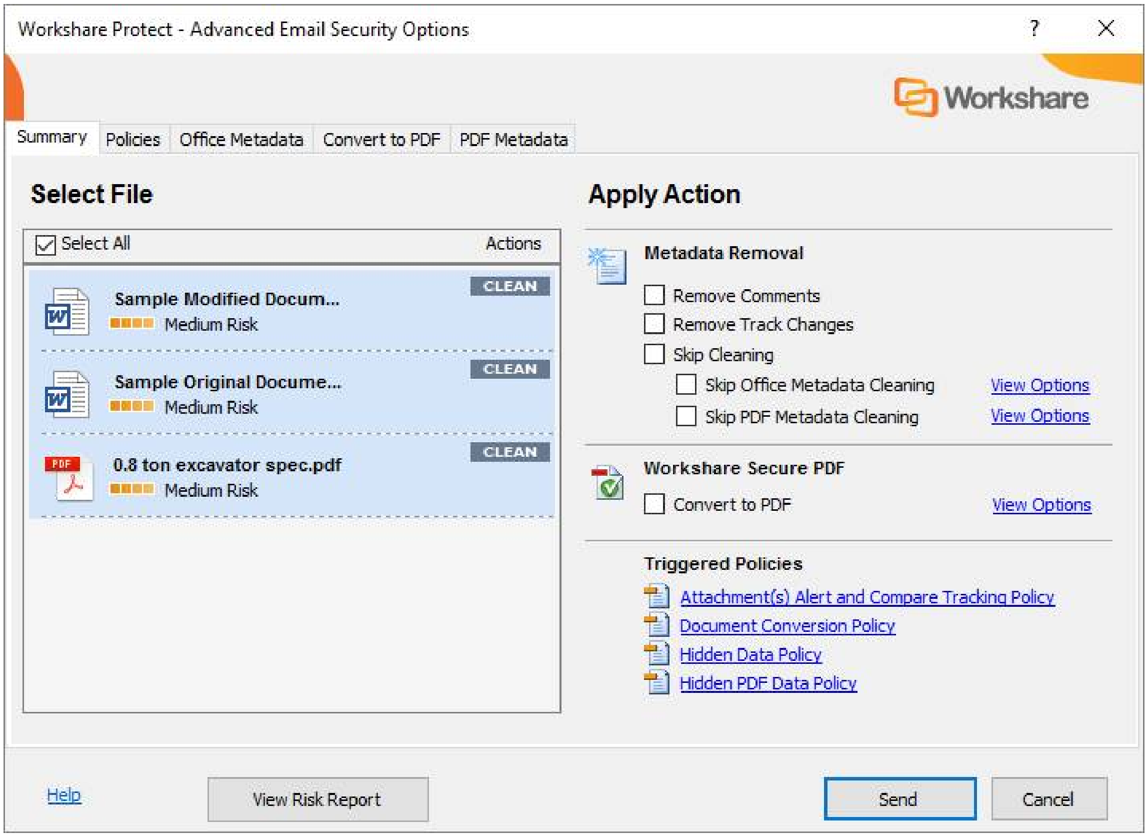
Clean & PDF
All metadata will be removed from Word, Excel, PowerPoint and P...

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

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

The Protect Profile dialog is described in *Using the Protect Profile Dialog*.

Email Security dialog



Workshare Protect - Advanced Email Security Options

Select File

☑ Select All — Actions

- Sample Modified Docum... — Medium Risk — CLEAN
- Sample Original Docume... — Medium Risk — CLEAN
- 0.8 ton excavator spec.pdf — Medium Risk — CLEAN

Apply Action

Metadata Removal

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

Workshare Secure PDF

□ Convert to PDF — View Options

Triggered Policies

- Attachment(s) Alert and Compare Tracking Policy
- Document Conversion Policy
- Hidden Data Policy
- Hidden PDF Data Policy

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

- **Email Security dialog 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. (For email to external recipients only, it is not displayed.) It is displayed after clicking **Send** once Workshare Protect has checked the email against the default profile.

> ***Note****: Workshare Protect must be turned on for internal email – select* ***Apply Workshare Protect*** *for* ***Internal Email*** *in the Workshare Configuration Manager (****Protection*** *>* ***Administration*** *category).*

- **Email Security dialog for external mail only**: The *Email Security* dialog is displayed when an email has external recipients. (For email to internal recipients only, it is not displayed.) It is displayed after clicking **Send** once Workshare Protect has checked the email against the default profile.

> ***Note**: Workshare Protect must be turned on for external email – select **Apply Workshare Protect** for **External Email** in the Workshare Configuration Manager (**Protection** > **Administration** category).*

- **No dialog (process actions transparently)**: The *Email Security* dialog is not displayed. Workshare Protect processes the email and applies the default profile without any user intervention.

The Email Security dialog is described in *Using the Email Security Dialog*.

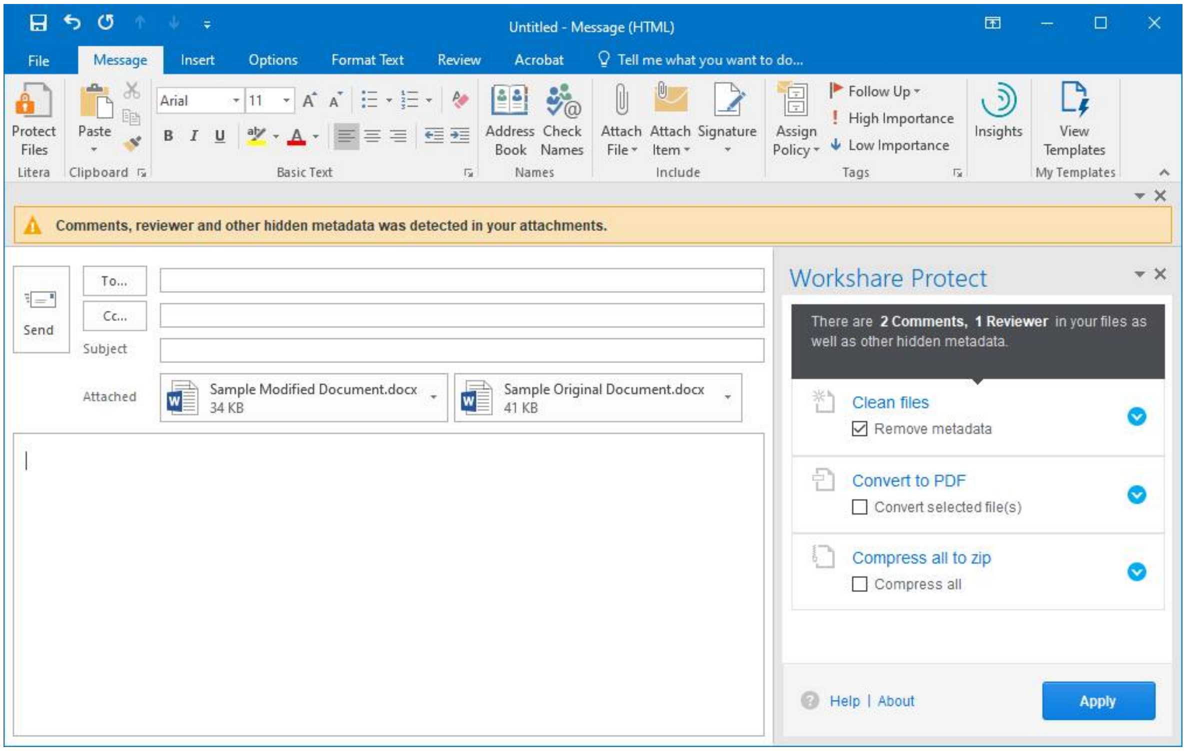
Using Interactive Protect

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

- **Clean files**: Enables you to clean metadata from your attachments.
- **Convert to PDF**: Enables you to convert attachments to PDF or PDF/A.
- **Compress all to zip**: Enables you to compress all attachments together into one zip file.

To work with Interactive Protect:

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



Comments, reviewer and other hidden metadata was detected in your attachments.

Attached: Sample Modified Document.docx 34 KB; Sample Original Document.docx 41 KB

There are **2 Comments, 1 Reviewer** in your files as well as other hidden metadata.

Clean files
☑ Remove metadata

Convert to PDF
□ Convert selected file(s)

Compress all to zip
□ Compress all

__Note__: If the Interactive Protect panel doesn’t open automatically, click the notification or click __Protect Files__ in the Message tab.

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

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

If you do NOT click **Apply** before sending the email, one of two things can happen:

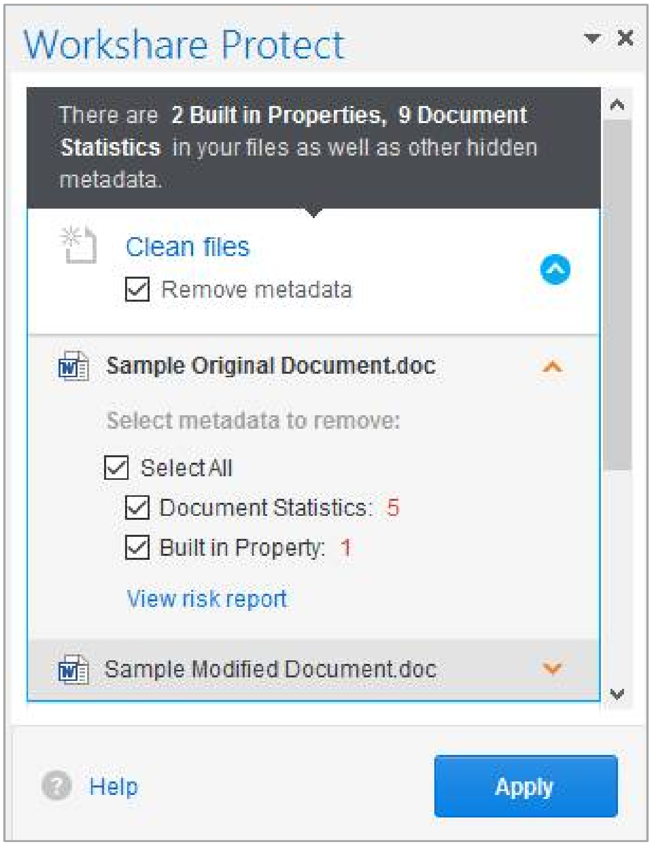
- If the parameter to automatically apply on send is selected in the Workshare Configuration Manager (**Protection**>**Interactive Protect** category), the Interactive Protect settings made in the panel will still be applied when you click **Send**.
- If the parameter is not selected, no processing will occur.

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

Cleaning metadata using Interactive Protect

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

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



Workshare Protect

There are **2 Built in Properties, 9 Document Statistics** in your files as well as other hidden metadata.

Clean files

☑ Remove metadata

Sample Original Document.doc

Select metadata to remove:

☑ Select All

☑ Document Statistics: 5

☑ Built in Property: 1

View risk report

Sample Modified Document.doc

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

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

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

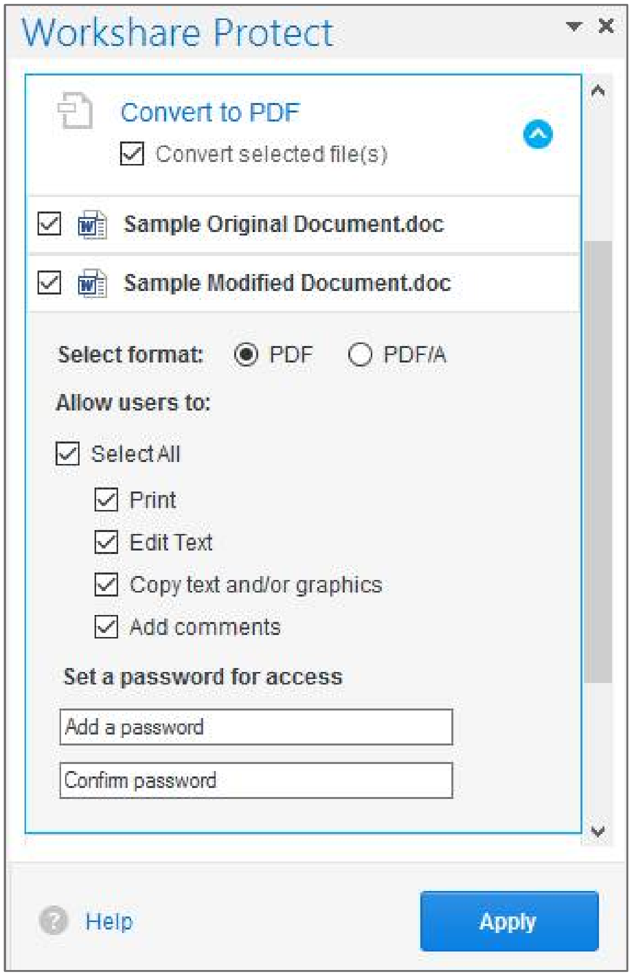
You can write your email while the attachments are being cleaned and then preview the files by opening the cleaned attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

Converting attachments to PDF using Interactive Protect

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

> ***Tip!*** *You can clean attachments before converting to PDF. You can also convert to PDF after converting your attachments to links.*

To select specific attachments to convert and to specify PDF conversion settings for the attachments, you can select the **Convert selected file(s)** checkbox and expand the **Convert to PDF** section.



Workshare Protect

Convert to PDF

☑ Convert selected file(s)

☑ Sample Original Document.doc

☑ Sample Modified Document.doc

Select format: ● PDF ○ PDF/A

Allow users to:

☑ Select All

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

Set a password for access

Add a password

Confirm password

- Deselect any attachments you do NOT want converting to PDF.

- Select whether to convert the attachments to PDF or PDF/A.
- Select all or some of the following security options:
  - **Print:** Enables recipients to print PDF files.
  - **Edit Text:** Enables recipients with Adobe Distiller to edit PDF files.
  - **Copy text and/or graphics:** Enables recipients to copy graphics or text directly from PDF files.
  - **Add comments:** Enables recipients with Adobe Distiller to add comments to PDF files.

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

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

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

Click **Apply** and the selected PDF settings are applied to all attachments that you have selected to convert to PDF.

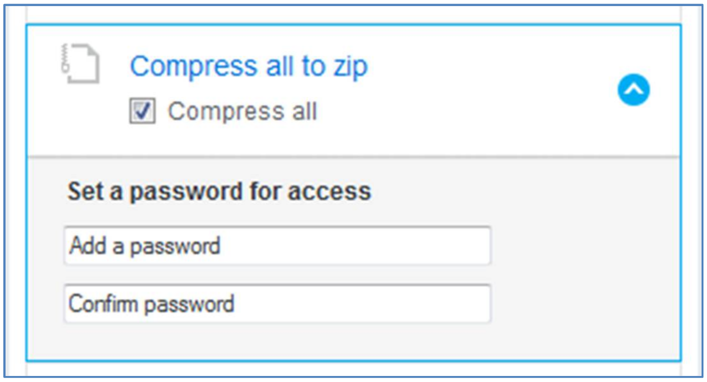
You can write your email while the attachments are being converted and then preview the files by opening the converted attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

Compressing attachments using Interactive Protect

In the Interactive Protect panel, you can select the **Compress all** checkbox in the **Compress all to zip** section and click **Apply** and all attachments are compressed into a single zip file.

Tip! *You can clean attachments before compressing.*

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



Compress all to zip

☑ Compress all

Set a password for access

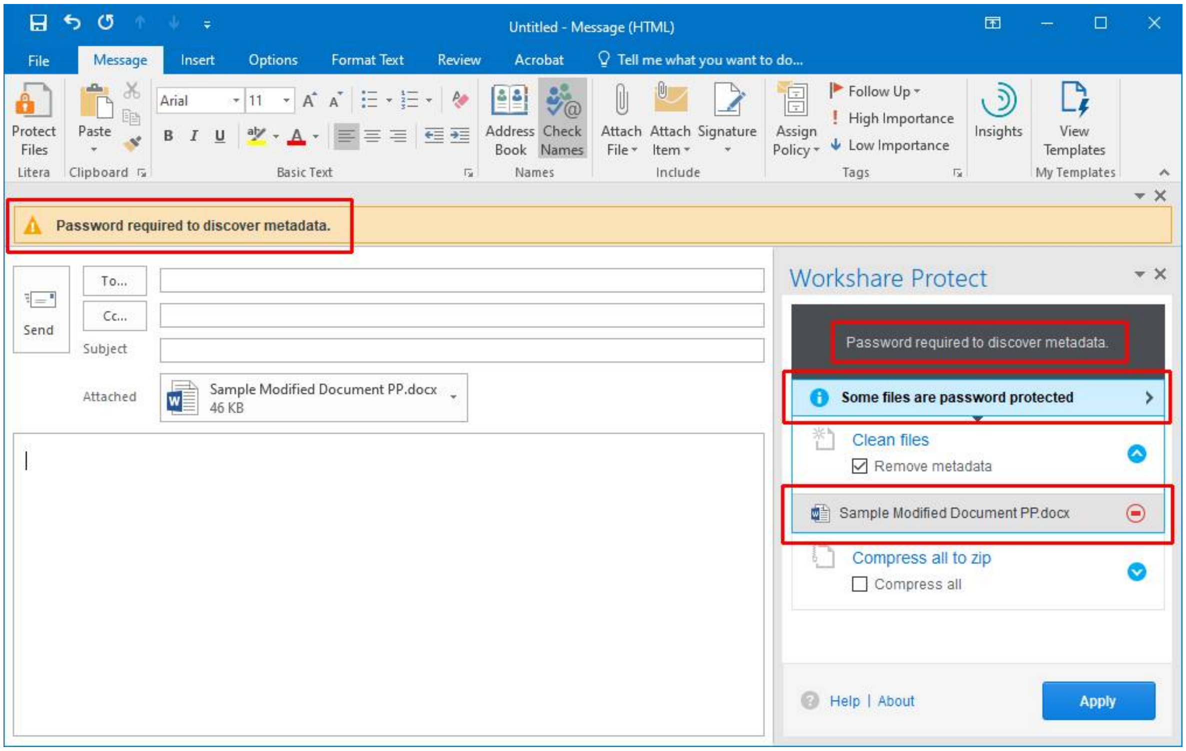
If required, set a password to protect the zip file by entering the password twice. When a password is specified, recipients can only open the zip file after entering this password.

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

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

Password-protected files and Interactive Protect

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



Password required to discover metadata.

Attached: Sample Modified Document PP.docx 46 KB

Password required to discover metadata.

Some files are password protected

Clean files

☑ Remove metadata

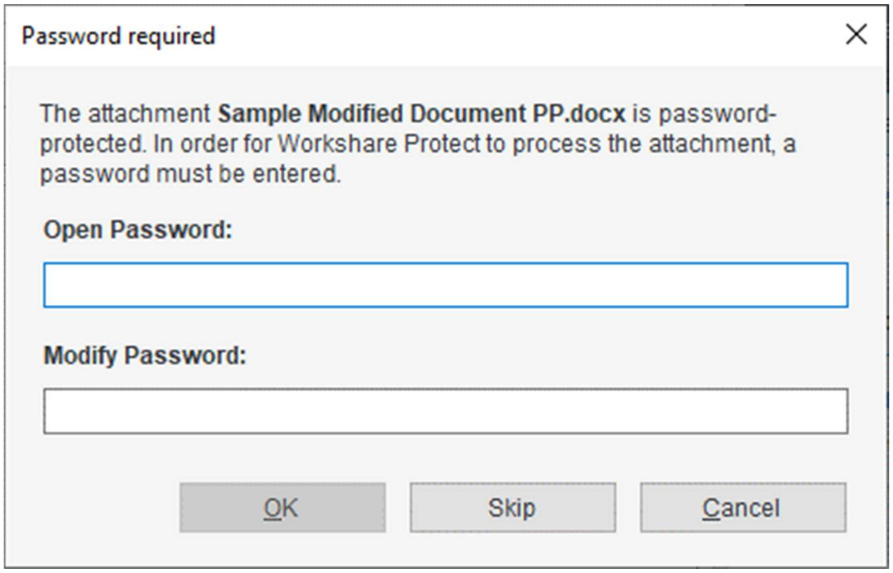
Sample Modified Document PP.docx

Compress all to zip

☐ Compress all

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

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



The attachment **Sample Modified Document PP.docx** is password-protected. In order for Workshare Protect to process the attachment, a password must be entered.

Open Password:

Modify Password:

Enter the open or modify passwords (or both) and click **OK**.

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

***Note**: You can compress password-protected attachments without the need to enter the open/modify password.*

Using the Protect Profile Dialog

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

A profile is a collection of policies that include a set of instructions to Workshare Protect as to what metadata to remove from an email attachment 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.

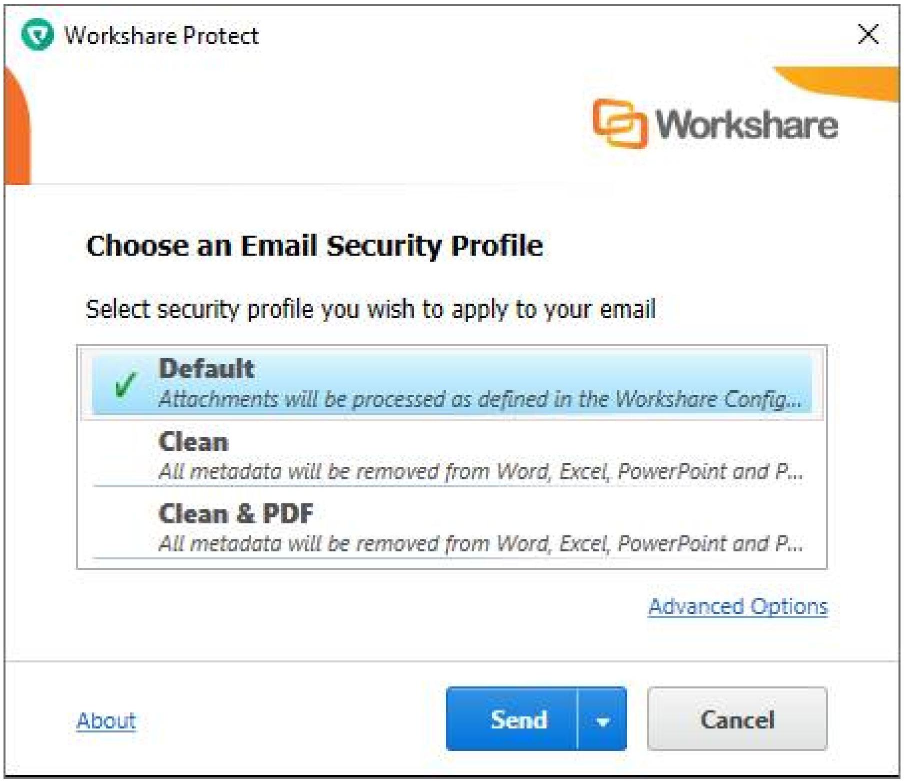
Your administrator defines profiles. Your administrator may have adopted a task-based approach or recipient-based approach when creating profiles:

- **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.



Choose an Email Security Profile

Select security profile you wish to apply to your email

- ✓ **Default**
  Attachments will be processed as defined in the Workshare Config...
- **Clean**
  All metadata will be removed from Word, Excel, PowerPoint and P...
- **Clean & PDF**
  All metadata will be removed from Word, Excel, PowerPoint and P...

2. Select the profile you want to apply to your attachments and click **Send**. The following 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 options matching the profile selected. Refer to *Using the Email Security Dialog*.

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

Using the Email Security Dialog

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

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

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

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

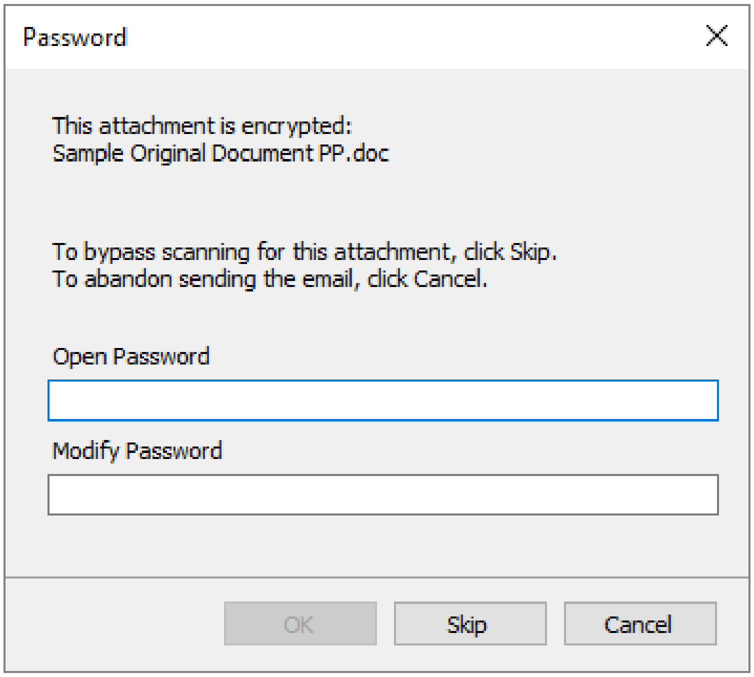
Note: *Workshare Protect will only check attachments of emails sent internally or externally (or both) if Workshare Protect is turned on for internal or external emails (or both). This is done using the* ***Apply Workshare Protect*** *parameter in the Workshare Configuration Manager (****Protection*** *>* ***Administration*** *category). 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 Microsoft Word where the user can set a password that must be entered in order to **open** or **modify** the document.

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

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



This attachment is encrypted:
Sample Original Document PP.doc

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

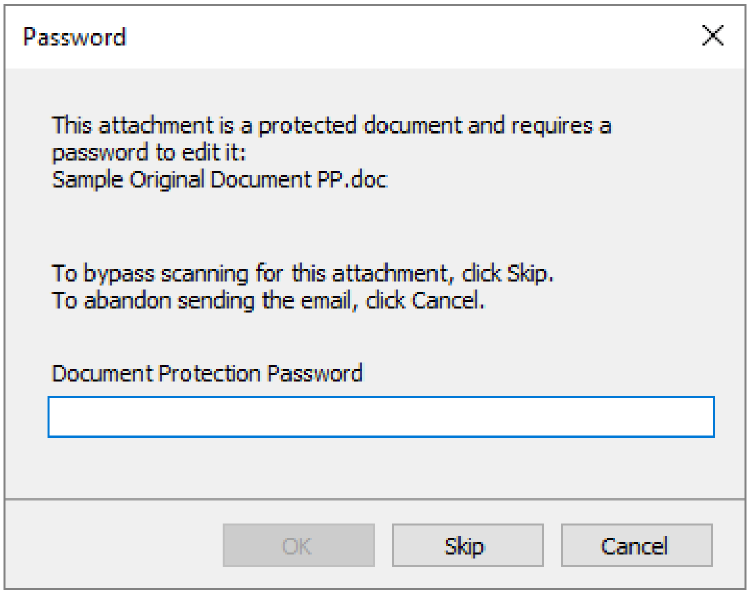
Enter the password required to open the document in the **Open Password** or **Modify Password** field and click **OK**, or you can click **Skip** and Workshare Protect will not check the document.

Protected documents

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 Microsoft Word where the user can restrict specific users from editing specific sections of the document. The protection settings are protected by a password.

***Note**: This functionality is available from the **Review** tab (**Protect** group) – click **Restrict Editing**.*

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



Password

This attachment is a protected document and requires a password to edit it:
Sample Original Document PP.doc

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

Document Protection Password

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

Send and Protect

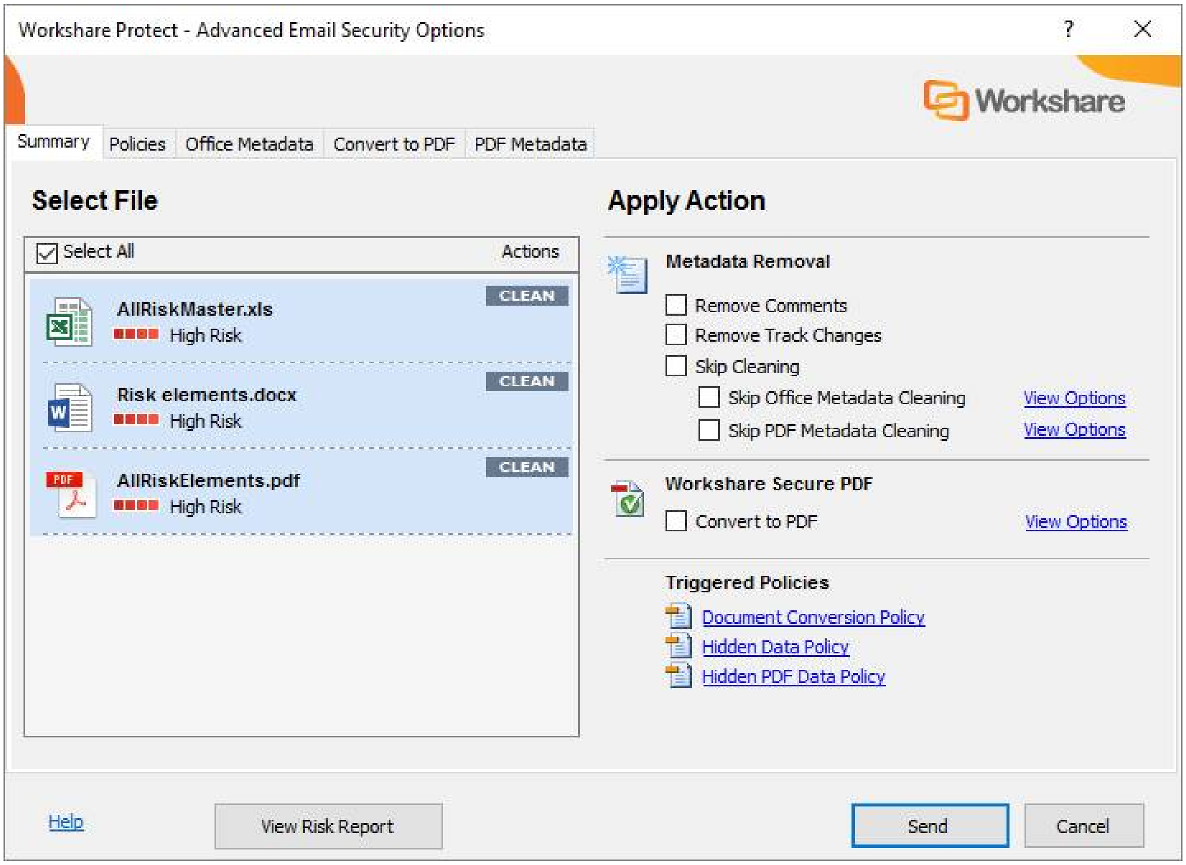
Your administrator may have configured Workshare Protect to include a **Send and Protect** button in your message window. If so, you can click this button instead of clicking **Send** and the *Email Security* dialog will always be displayed – regardless of how the **When sending an email with attachments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

Sending emails

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

To send an email:

Create a new email, attach the required document(s) and click **Send**. Workshare Protect checks the email against the default profile and the *Email Security* dialog is displayed.



☑ Select All — Actions

AllRiskMaster.xls — High Risk — CLEAN

Risk elements.docx — High Risk — CLEAN

AllRiskElements.pdf — High Risk — CLEAN

Metadata Removal

☐ Remove Comments

☐ Remove Track Changes

☐ Skip Cleaning

☐ Skip Office Metadata Cleaning — View Options

☐ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

☐ Convert to PDF — View Options

Triggered Policies

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

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.

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

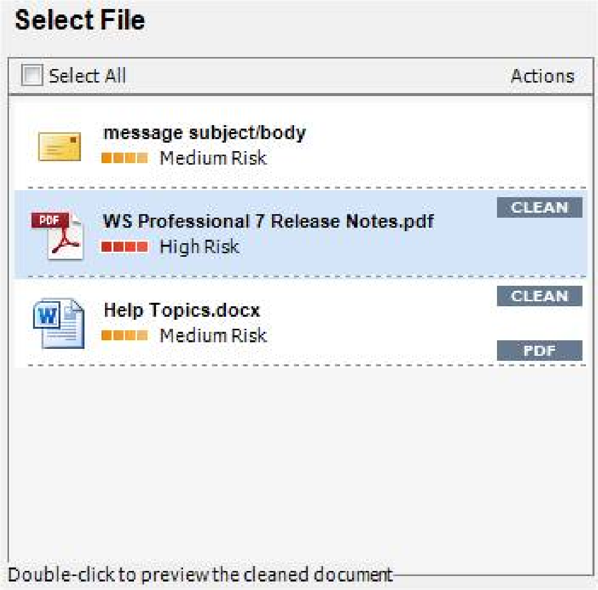
Quick tour of the Email Security dialog

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

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

Select File area

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



Select File

□ Select All Actions

message subject/body
■■■■ Medium Risk

WS Professional 7 Release Notes.pdf
■■■■ High Risk
CLEAN

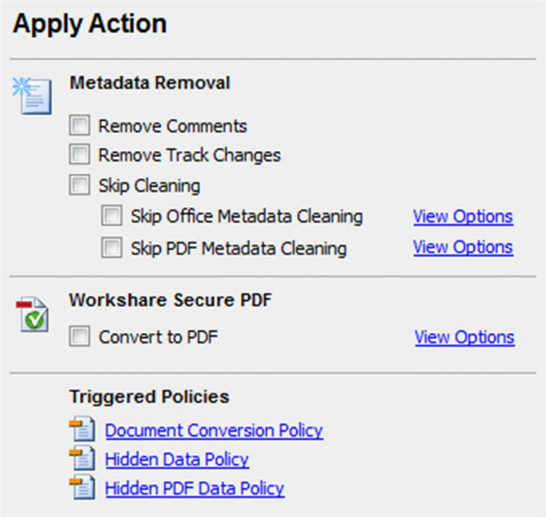
Help Topics.docx
■■■■ Medium Risk
CLEAN
PDF

Double-click to preview the cleaned document

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

Summary tab

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



Apply Action

Metadata Removal

□ Remove Comments

□ Remove Track Changes

□ Skip Cleaning

□ Skip Office Metadata Cleaning View Options

□ Skip PDF Metadata Cleaning View Options

Workshare Secure PDF

□ Convert to PDF View Options

Triggered Policies

Document Conversion Policy

Hidden Data Policy

Hidden PDF Data Policy

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

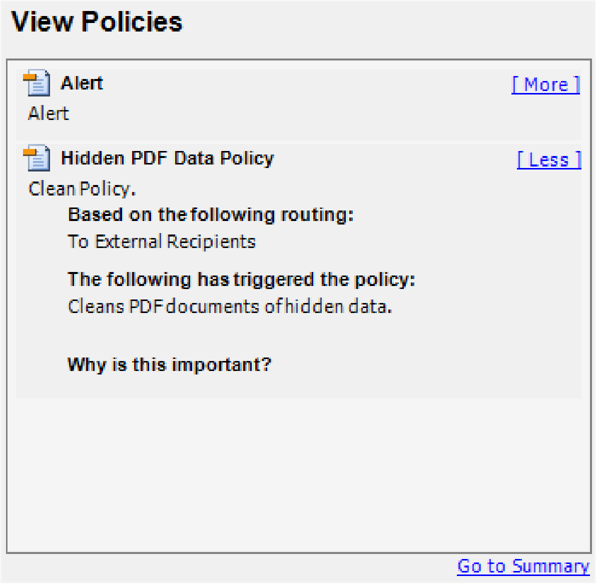
Under **Workshare Secure PDF**, selecting **Convert to PDF** means the selected attachment is converted into PDF. Click **View Options** to display all options in the **Convert to PDF** tab.

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

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

Policies tab

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



View Policies

Alert

Alert

Hidden PDF Data Policy

Clean Policy.

Based on the following routing:

To External Recipients

The following has triggered the policy:

Cleans PDF documents of hidden data.

Why is this important?

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 PDF Clean action is triggered for a PDF file. Refer to *Cleaning hidden data from attachments,* for more information.

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

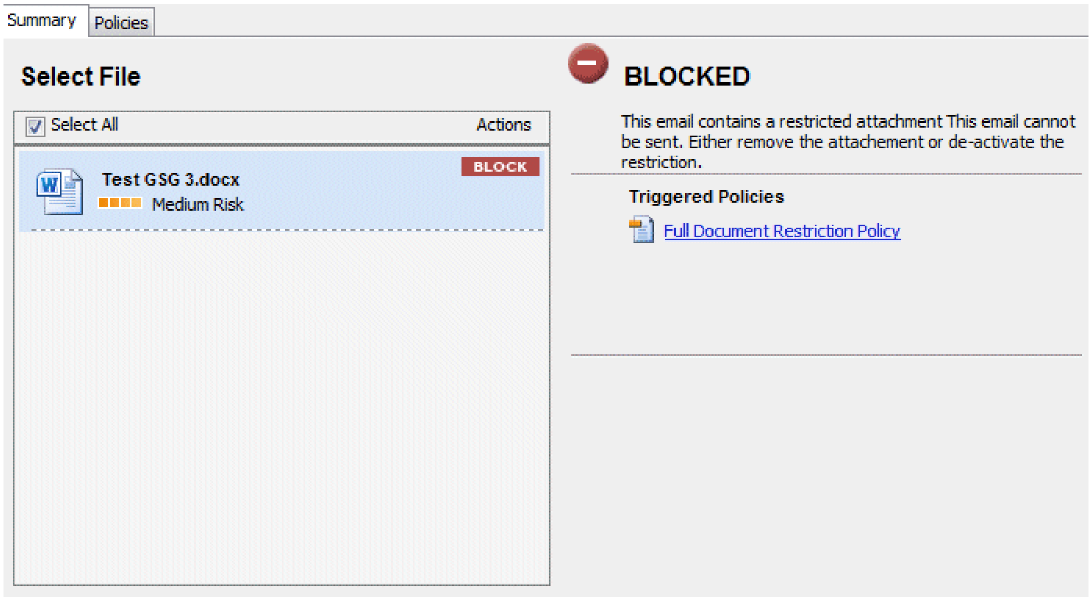
The **ZIP Options** tab is included in the *Email Security* dialog when a Zip action is triggered.

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.



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

To resolve blocked emails:

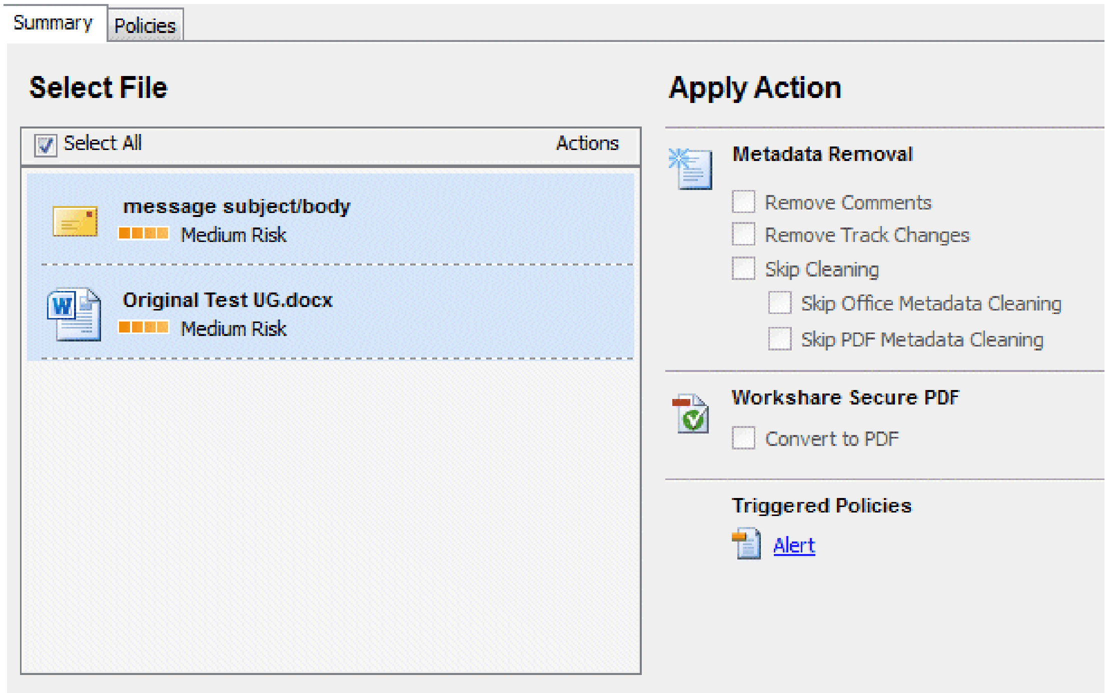
1. Click the name of the policy in the **Triggered Policies** list or select the **Policies** tab to view what content has triggered the email policy.
2. Click the **Close** button to close the *Email Security* dialog.
3. Make the appropriate changes to the email and/or document(s) by removing or modifying 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.



Summary | Policies

Select File

☑ Select All — Actions

message subject/body — Medium Risk

Original Test UG.docx — Medium Risk

Apply Action

Metadata Removal

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

Workshare Secure PDF

□ Convert to PDF

Triggered Policies

Alert

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

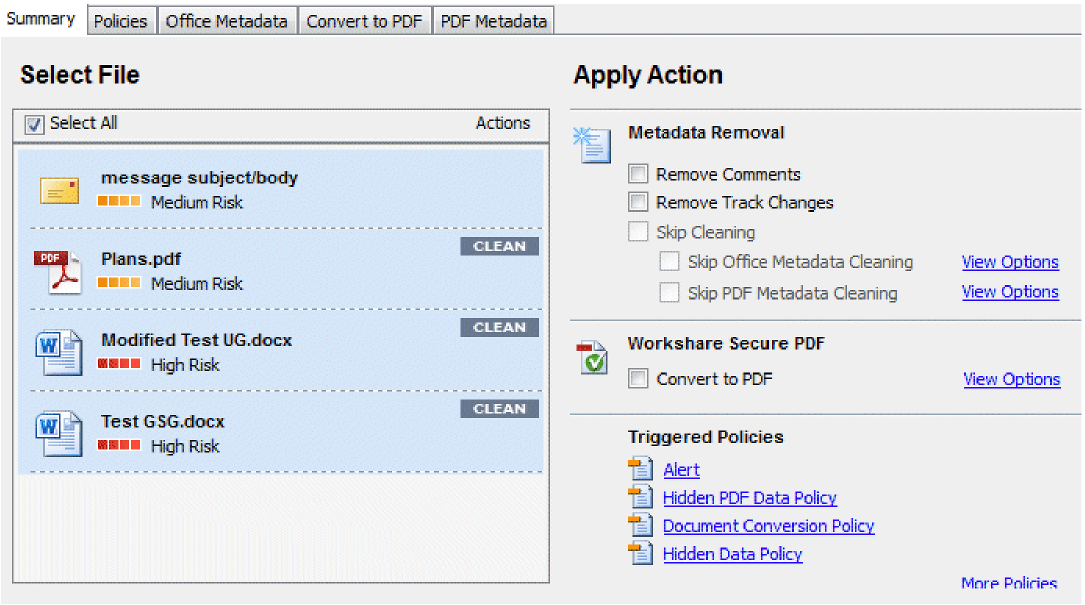
When you are ready to send the email, click **Send**.

Cleaning hidden data from attachments

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

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

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



Summary | Policies | Office Metadata | Convert to PDF | PDF Metadata

Select File

☑ Select All — Actions

message subject/body — Medium Risk

Plans.pdf — Medium Risk — CLEAN

Modified Test UG.docx — High Risk — CLEAN

Test GSG.docx — High Risk — CLEAN

Apply Action

Metadata Removal

□ Remove Comments

□ Remove Track Changes

□ Skip Cleaning

□ Skip Office Metadata Cleaning — View Options

□ Skip PDF Metadata Cleaning — View Options

Workshare Secure PDF

□ Convert to PDF — View Options

Triggered Policies

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

More Policies

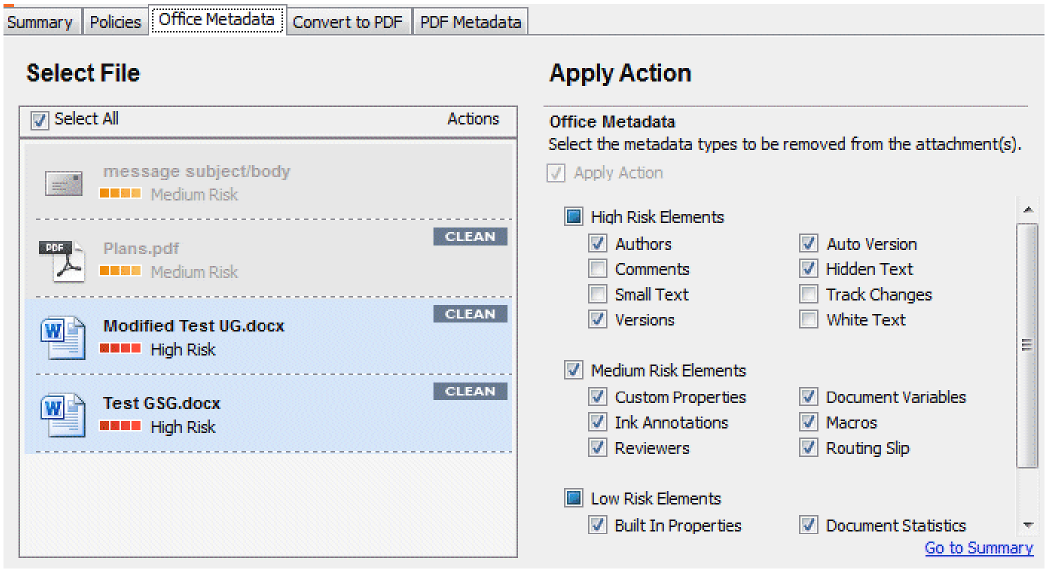
***Note:** For more information on the types of hidden data contained within Microsoft Office documents, see* Cleaning options*.*

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

To clean hidden data:

1. Select the attachment in the **Select File** list to specify individual options for a single attachment or select the **Select All** checkbox to select all attachments. Any settings will then be applied to all attachments.

2. Click **View Options** in the **Metadata Removal** area or select the **Office Metadata** tab. The **Office Metadata** tab displays the different hidden data cleaning options for Microsoft Office attachments.



Select File

☑ Select All — Actions

message subject/body — Medium Risk

Plans.pdf — Medium Risk

Modified Test UG.docx — High Risk

Test GSG.docx — High Risk

Apply Action

Office Metadata
Select the metadata types to be removed from the attachment(s).
☑ Apply Action

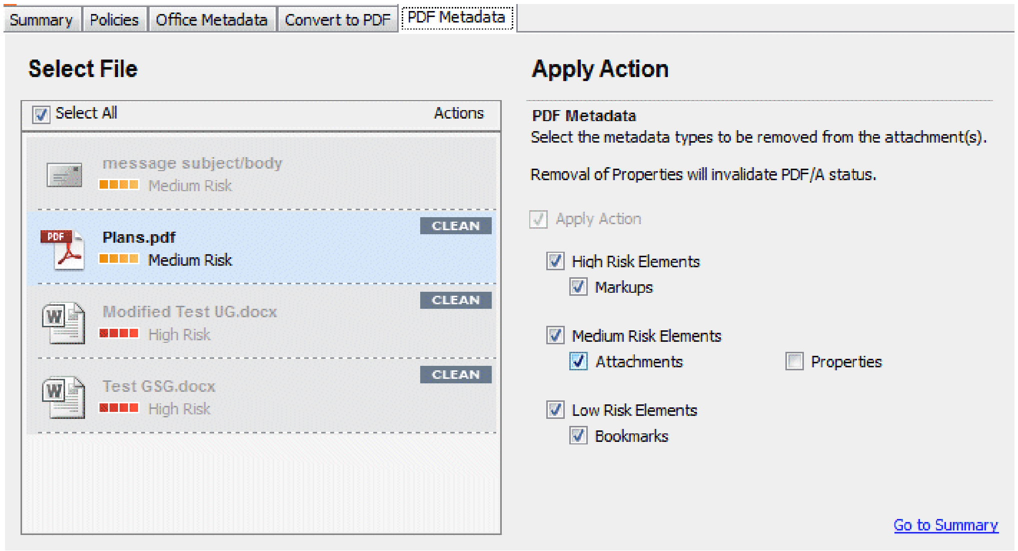
■ High Risk Elements
☑ Authors ☑ Auto Version
□ Comments ☑ Hidden Text
□ Small Text □ Track Changes
☑ Versions □ White Text

☑ Medium Risk Elements
☑ Custom Properties ☑ Document Variables
☑ Ink Annotations ☑ Macros
☑ Reviewers ☑ Routing Slip

■ Low Risk Elements
☑ Built In Properties ☑ Document Statistics

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

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



Select File

☑ Select All — Actions

message subject/body — Medium Risk

Plans.pdf — Medium Risk

Modified Test UG.docx — High Risk

Test GSG.docx — High Risk

Apply Action

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

Removal of Properties will invalidate PDF/A status.

☑ Apply Action

☑ High Risk Elements
☑ Markups

☑ Medium Risk Elements
☑ Attachments □ Properties

☑ Low Risk Elements
☑ Bookmarks

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

> ***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.*

6. Repeat for additional attachments if required.
7. Click **Send** to send the email.

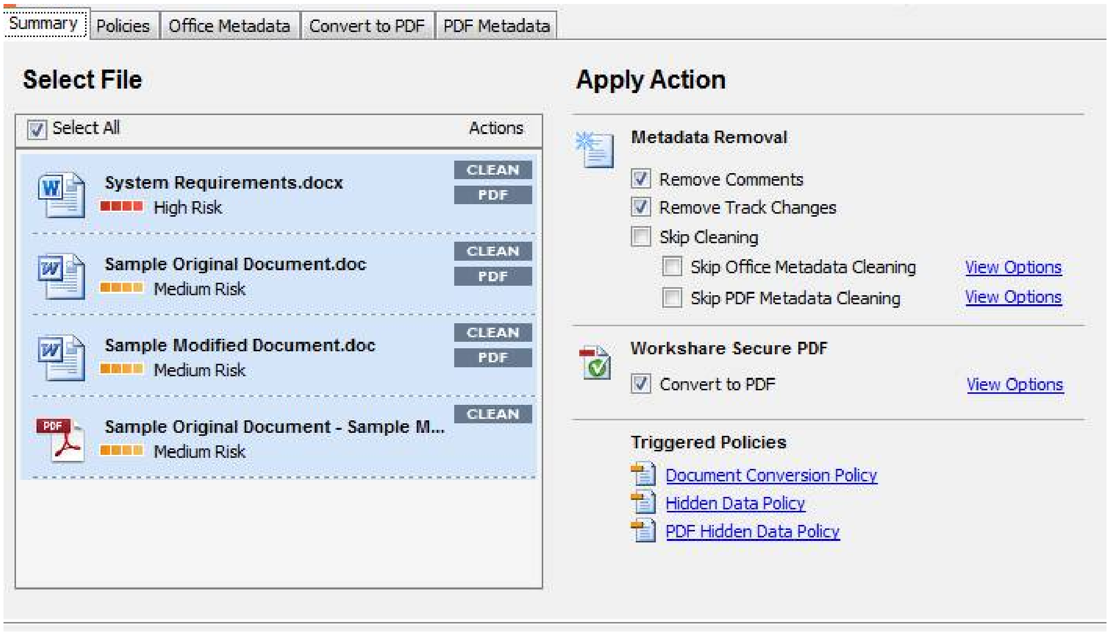
Workshare Protect cleans the hidden data from the attached document(s) according to your settings before sending the email.

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.



Select File

☑ Select All

System Requirements.docx — High Risk
Sample Original Document.doc — Medium Risk
Sample Modified Document.doc — Medium Risk
Sample Original Document - Sample M... — Medium Risk

Apply Action

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

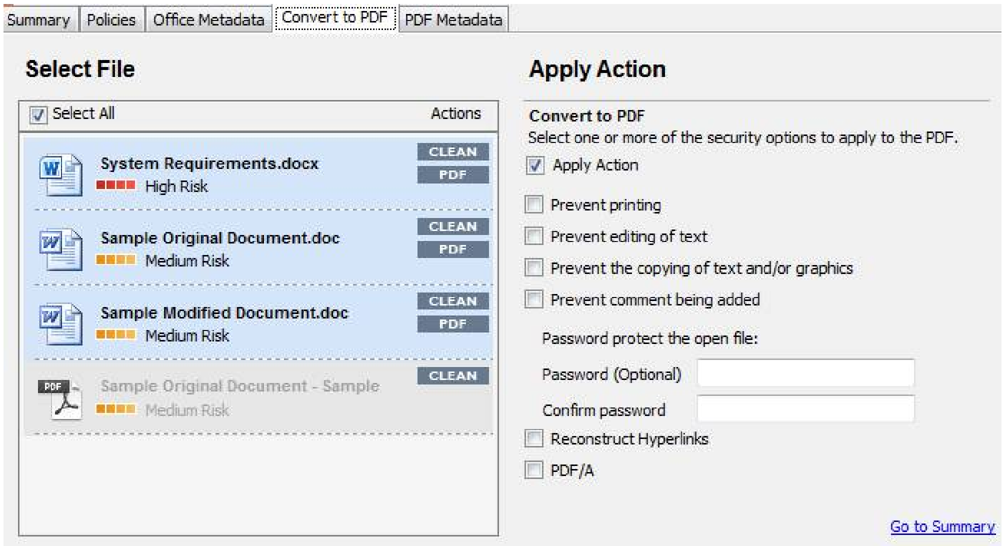
Workshare Secure PDF
☑ Convert to PDF

Triggered Policies
Document Conversion Policy
Hidden Data Policy
PDF Hidden Data Policy

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

To convert attachments to PDF:

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



Select File

☑ Select All — Actions

- System Requirements.docx — High Risk
- Sample Original Document.doc — Medium Risk
- Sample Modified Document.doc — Medium Risk
- Sample Original Document - Sample — Medium Risk

Apply Action

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

☑ Apply Action

☐ Prevent printing
☐ Prevent editing of text
☐ Prevent the copying of text and/or graphics
☐ Prevent comment being added

Password protect the open file:
Password (Optional)
Confirm password

☐ Reconstruct Hyperlinks
☐ PDF/A

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

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

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

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

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

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

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

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

Chapter 4: Advanced PDF Functionality

This chapter describes how to combine several documents into a single PDF. It includes the following section:

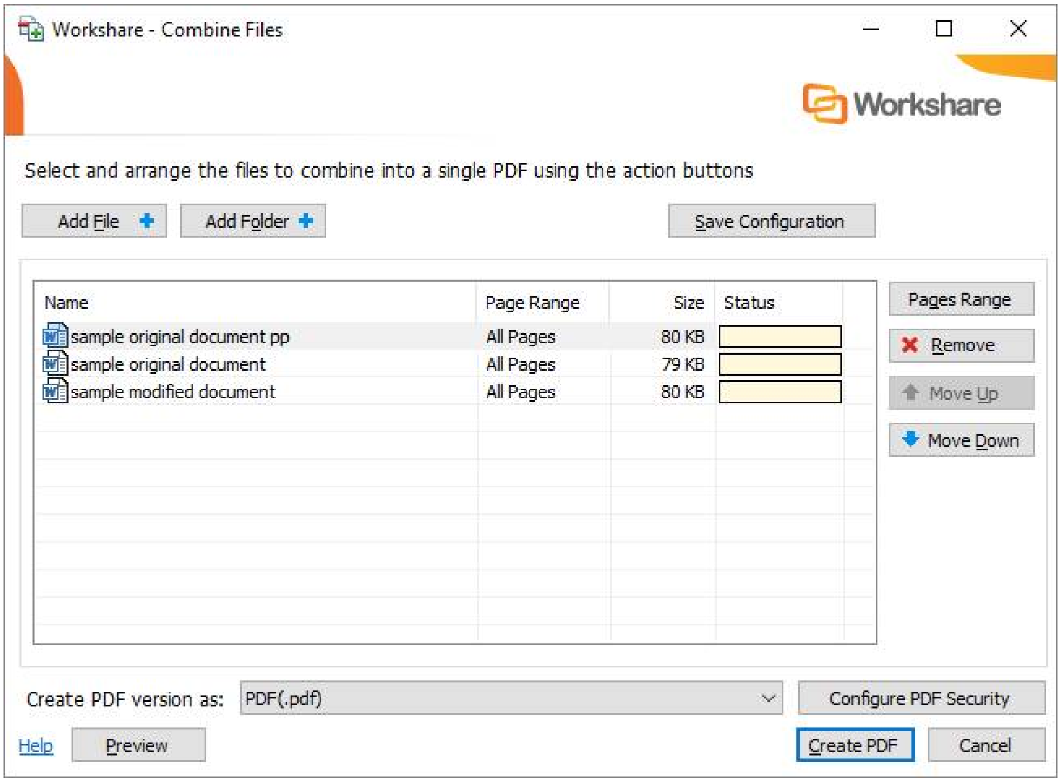
- **PDF Combine**, page 58, describes how to combine multiple files into a single PDF.

PDF Combine

Workshare Protect enables you to combine multiple files into a single PDF or PDF/A file. For example, electronic court submissions are required to be submitted as a PDF or PDF/A file. Case information can include multiple file formats such as contracts, financial spreadsheets and email conversations. You can combine a range of file types including Word, Excel, PowerPoint, PDF, RTF, TXT, HTML, MSG and other formats.

To combine multiple documents into a single PDF:

1. In an open Office document, click **Combine PDF** (**Protect** group) in the Litera tab or in File Explorer or your DMS, right-click one or more files that you want to combine into a single PDF and select **Combine files in Workshare**. (You do not have to select all the files to combine at this stage but can add them later.) The *Combine Files* dialog is displayed.



Select and arrange the files to combine into a single PDF using the action buttons

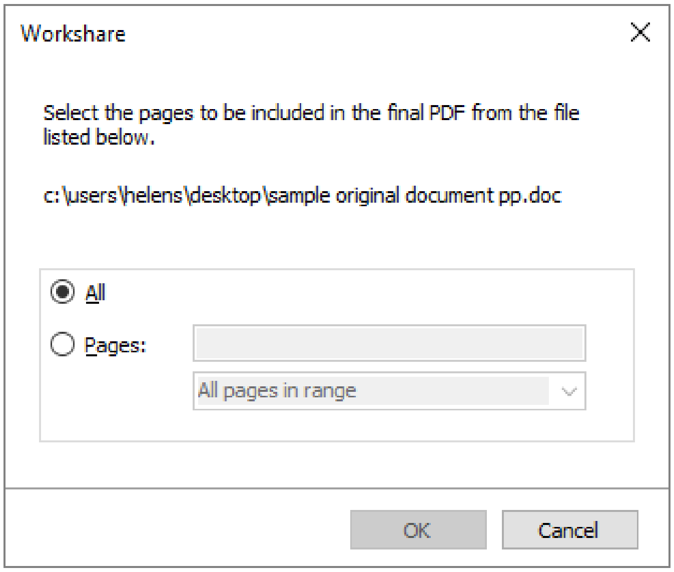
Name	Page Range	Size	Status
sample original document pp	All Pages	80 KB	
sample original document	All Pages	79 KB	
sample modified document	All Pages	80 KB	

Create PDF version as: PDF(.pdf)

2. Add the additional files you want to include in the single PDF using the buttons at the top or by dragging and dropping. Click **Add Files** to select and add a single file and click **Add Folder** to add multiple files from a selected folder.

3. Once you have selected the files to combine, arrange the order using the **Move Up** and **Move Down** buttons. If you want to remove a file from the list, select it and click **Remove**.

4. If you only want to include selected pages from a particular document, select the file in the list and click **Pages Range**.



Workshare

Select the pages to be included in the final PDF from the file listed below.

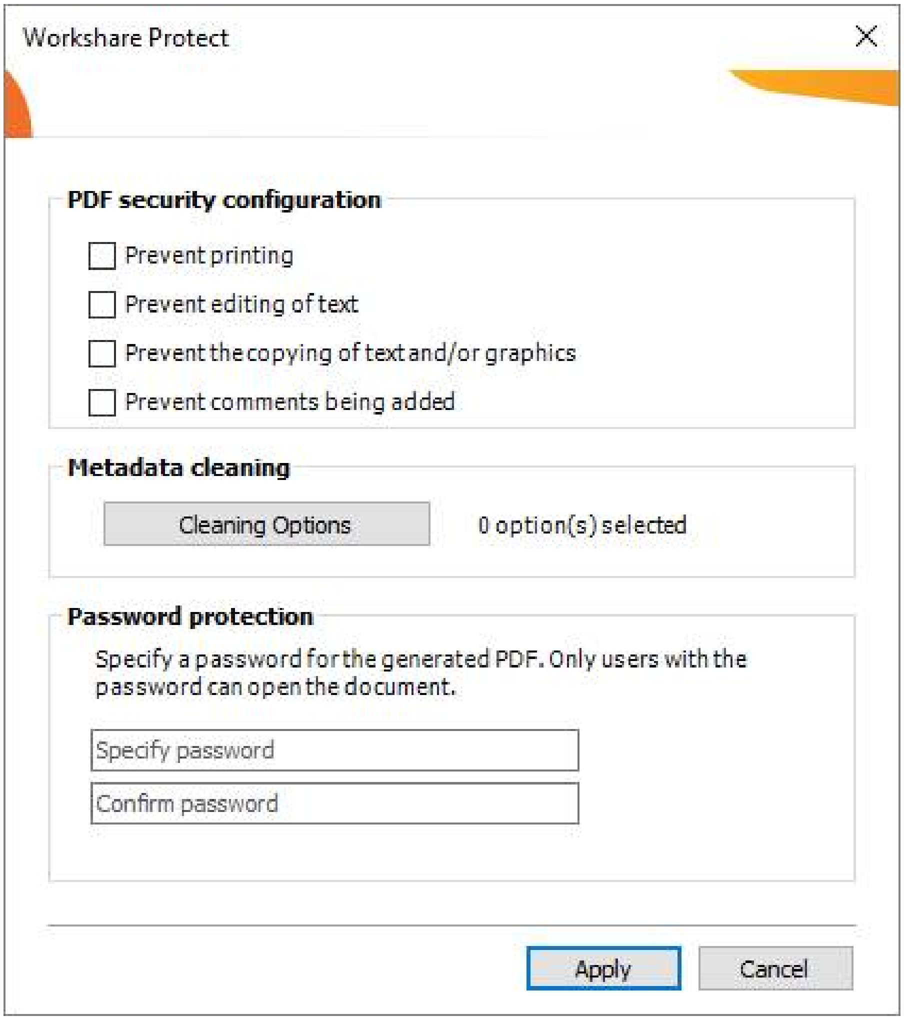
c:\users\helens\desktop\sample original document pp.doc

● All

○ Pages:

5. Select the **Pages** radio button and specify the pages to be included into the combined PDF as required.
6. Click **OK**.
7. Select whether you want to create a PDF file or a PDF/A file from the **Create PDF version as** dropdown list.

8. If you want to set security options for the combined PDF, click **Configure PDF Security**.



Workshare Protect

PDF security configuration

□ Prevent printing

□ Prevent editing of text

□ Prevent the copying of text and/or graphics

□ Prevent comments being added

Metadata cleaning

Cleaning Options 0 option(s) selected

Password protection

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

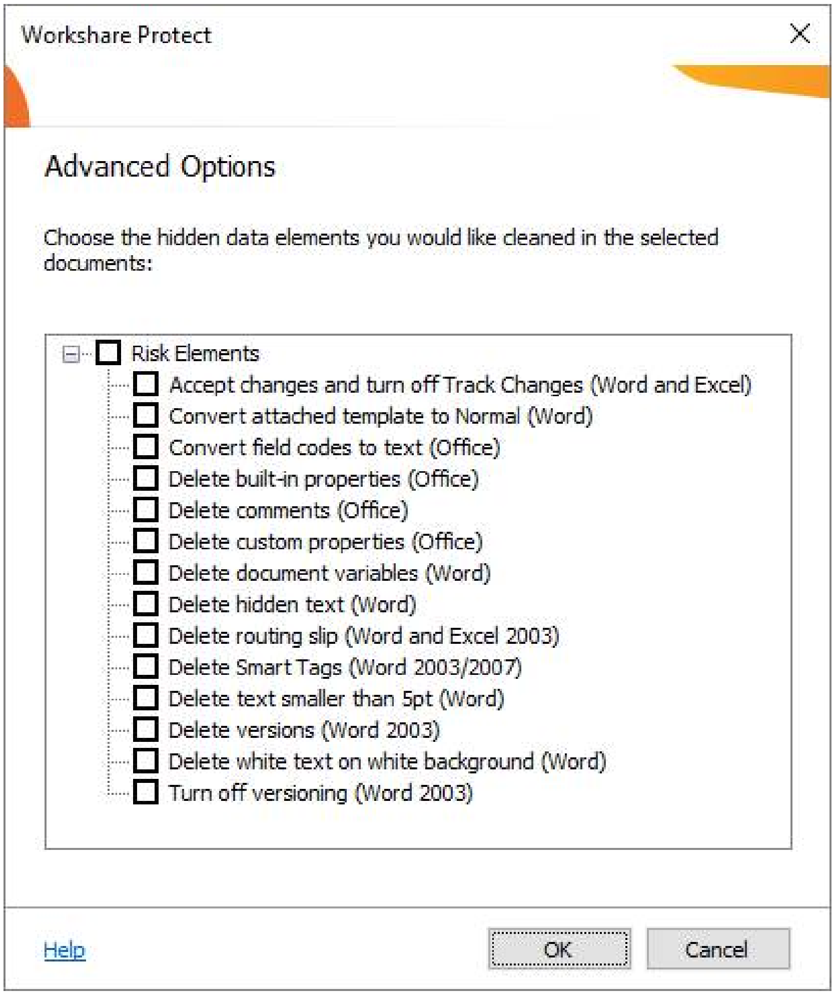
Specify password

Confirm password

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

Note: *These options are disabled and cannot be selected if you selected PDF/A in step 7.*

10. To specify what hidden data to remove before converting it to PDF, select the **Clean before PDF** checkbox and click **Cleaning Options**.



Workshare Protect

Advanced Options

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

- □ Risk Elements
  - □ Accept changes and turn off Track Changes (Word and Excel)
  - □ Convert attached template to Normal (Word)
  - □ Convert field codes to text (Office)
  - □ Delete built-in properties (Office)
  - □ Delete comments (Office)
  - □ Delete custom properties (Office)
  - □ Delete document variables (Word)
  - □ Delete hidden text (Word)
  - □ Delete routing slip (Word and Excel 2003)
  - □ Delete Smart Tags (Word 2003/2007)
  - □ Delete text smaller than 5pt (Word)
  - □ Delete versions (Word 2003)
  - □ Delete white text on white background (Word)
  - □ Turn off versioning (Word 2003)

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

12. Click **OK**.

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

> *Note: If you selected PDF/A in step 7, you cannot set a password and the Password protection area is disabled.*

14. Click **Apply**.

15. If required, click **Preview** to view the combined PDF.

16. Click **Create PDF**. A *Save as* dialog is displayed.

17. Specify the name and location for the combined PDF file and click **Save**. The documents are converted into a single PDF. The progress of the operation can be seen in the **Status** column in the *Combine files* dialog.

If you want to save your selection without creating a PDF – for example, if you have not completed the selection of documents – you can save your work in progress as a Workshare workbook (.WWB) by clicking **Save** in the *Combine Files* dialog. When you are ready to work on it again, simply right-click the WWB file and select **Combine files in Workshare** or drag new files you want to include over the WWB file. This re-opens the *Combine Files* dialog and you can continue.

***Note**: For iManage users, in order to save a Workshare workbook, the WWB file type needs to be registered as a file type on the Worksite Server.*

Chapter 5: Configuring Workshare

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

- **Introducing the Workshare Configuration Manager**, page 64, introduces the Workshare configuration utility.
- **Accessing the Workshare Configuration Manager**, page 64, describes how to access the Workshare Configuration Manager.
- **Setting Parameters**, page 66, 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 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.

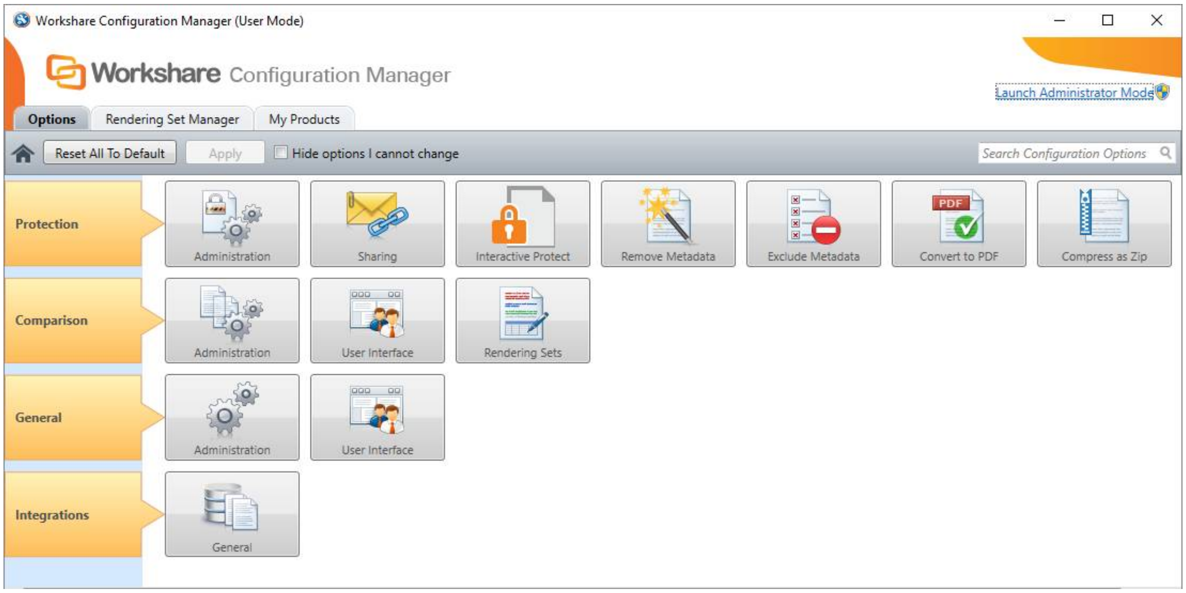
***Note:** Your system administrator may have restricted the rights of users to modify configuration parameters by locking individual parameters so that users cannot override the setting. If you have restricted access rights and have special requirements for configuration, please speak to your system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

Accessing the Workshare Configuration Manager

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

To access the Workshare Configuration Manager:

In an open document, click **Options** in the Litera tab or from the Start menu, select **Workshare Configuration (User Mode)**. The Workshare Configuration Manager opens in User Mode.

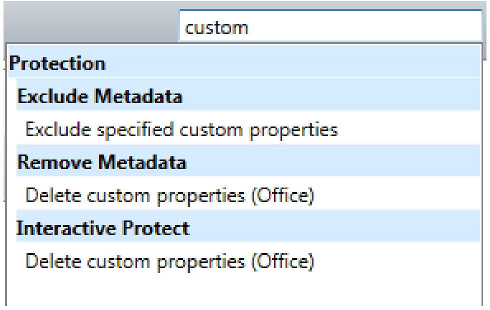


Note: In User Mode, the state of the options reflects the settings in HKEY_CURRENT_USER in the Registry.

The configuration parameters for Workshare are grouped into categories and sub-categories. Click a sub-category to display its parameters. The different sub-categories and their parameters are described in a separate guide - *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.



custom

Protection

Exclude Metadata

Exclude specified custom properties

Remove Metadata

Delete custom properties (Office)

Interactive Protect

Delete custom properties (Office)

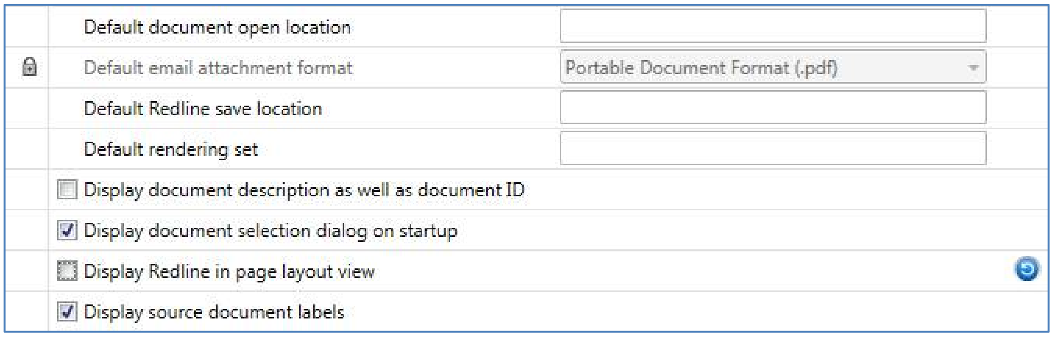
Click the parameter in the results list and the relevant category and sub-category is displayed in the Workshare Configuration Manager.

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.



Default document open location

🔒 Default email attachment format — Portable Document Format (.pdf)

Default Redline save location

Default rendering set

□ Display document description as well as document ID

☑ Display document selection dialog on startup

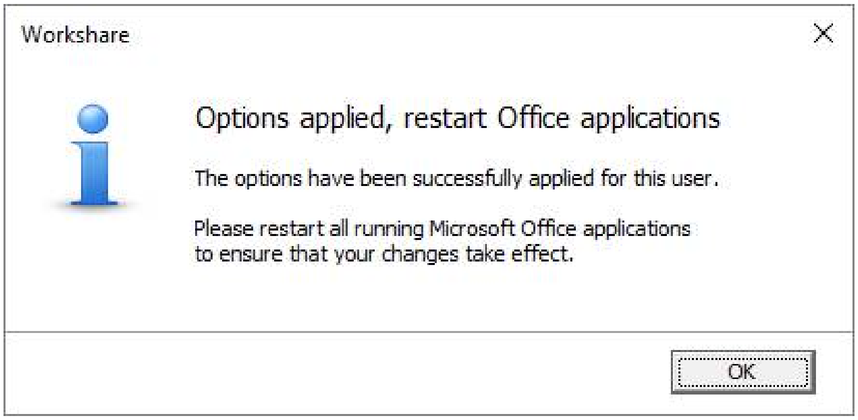
□ Display Redline in page layout view ↻

☑ Display source document labels

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

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

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



Workshare

Options applied, restart Office applications

The options have been successfully applied for this user.

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

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

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

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

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

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

Revisions
Published for Workshare Protect 10: 18/12/18; minor revisions: 17/1/19 & 15/2/19
Revised for Workshare Protect 10.1: 27/3/19
Revised for Workshare Protect 10.1 Revision 1: 16/5/19
Revised for Workshare Protect 10.2: 28/6/19
Revised for Workshare Protect 10.2 Revision 1: 19/8/19
Revised for Workshare Protect 10.3: 2/10/19
Revised for Workshare Protect 10.4: 09/12/19

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