Workshare Protect 9.5

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 7, introduces Workshare Protect.
- **Workshare Protect Functionality**, page 7, describes the different areas of functionality of Protect.
- **Accessing Protect Functionality**, page 10, describes how to access Protect functionality after install.
- **Licensing**, page 13, 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/PDF creation/secure file transfer for attachments in Outlook
- Comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well as visible sensitive data
- Options to save and share Office documents to Workshare online
- Access and visibility into online collaborative workspaces directly from Office
- Secure file sharing from all devices and browsers with metadata removal and end-to-end encryption
- Centralized policy design and enforcement administrator tools
- Centralized user account management and control
- Complete access to Workshare online functionality to share and collaborate on documents, including setting folder access and permissions, positional commenting and reviewer communications with presence indicators
- Desktop sync app to synchronize your online content to your local desktop

***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.

Workshare Protect may include the Connect product to extend its functionality to Workshare online.

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. Additionally, users can securely transfer attachments to a secure location in Workshare online and send recipients a link to that location.

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).

File share and sync

Workshare's online services provide a secure file sharing and online collaboration tool that enables users to store, share, and collaborate on content. There are several ways of interacting with the online services offered by Workshare, either online through a web browser or using special apps. The Workshare desktop app is the app for use on PCs and it is installed as part of the Protect installation when you select the file share & sync option.

Note: Workshare's mobile app is an app designed for use on smartphones and tablets that provides access to documents in Workshare online while on the move.

Users can sync documents safely across all their devices automatically updating content between Workshare online and their desktop and mobile devices.

With the Groups functionality, users can easily organize and manage files and projects, ensuring the correct users and permissions are set up for a group. Tools for commenting, annotating, and file comparison are available to support all stages of document evolution. Users receive updates when files in particular groups are being accessed, commented on, or modified by other reviewers, so ideas and conversations are never missed. Once new file versions are uploaded, users can compare old and new versions to see at a glance what has changed.

Users can access, review, and collaborate on files from any device, supporting company-wide mobility initiatives. Users can also select files to save for offline access, enabling users to work on files without Internet access. Once the device is connected again, all updates are synced back as a new version.

IT security controls are available at an account level, allowing data governance regulations to be met, and reduce the risk of accidental data loss. For added security, organizations can choose where their corporate data is stored (public cloud, custom public cloud, or hybrid). Finally, Workshare online can be integrated with existing DMS to securely mobilize content, and get the most out of IT system investments.

With Protect, users can save and share Office files (directly from Office) to Workshare online so they can access them on their other devices and on the move. Once shared, users can see their shared document, spreadsheet or presentation come alive and understand who's reviewing it online- directly from Word, Excel or PowerPoint.

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	Share Point	NetDocuments	OpenText	Worldox
Convert to PDF (from Workshare tab)	✓	✓	✗	✓	✓
Combine PDF (from Workshare tab)	✓	✓	✗	✓	✓
Right-click: Convert to PDF with Workshare	✓	✗	✗	✓	✓
Right-click: Combine files in Workshare	✓	✗	✗	✓	✓
Browse from desktop app to add files to 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 Workshare 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 documents and select **Convert to PDF with Workshare** or **Combine files in Workshare** or **Send to/Workshare Batch Clean**.

- Right-click closed 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**.

- Right-click any file and select **Workshare/Share to Group**.

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

Start menu

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

- Under Workshare:
  - Workshare Batch Clean
  - Workshare Configuration (User Mode)
  - Workshare Configuration Assistant
  - Help
- Under Workshare Desktop
  - Workshare

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 tab

In Office applications, the Workshare tab is included as follows:
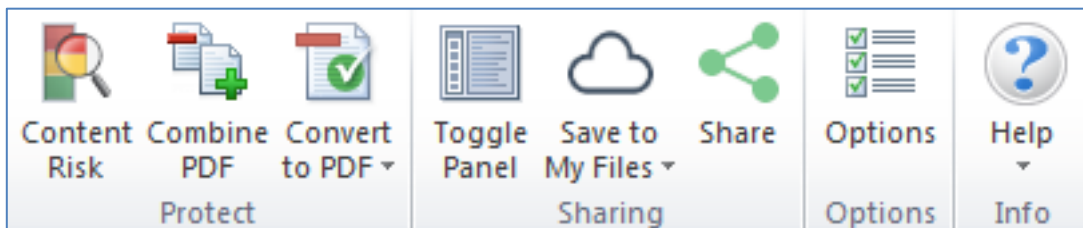

Whether these options are included in the tab is configurable from the **General > User Interface** category in the Workshare Configuration Manager. Refer to *Workshare Configuration Options* for further information.

The Workshare tab includes the following options:

| Group	Item	Description
Protect	**Content Risk**	Enables you to display a report of all the content risk in a document as well as remove selected hidden data from the document. Refer to *Displaying Content Risk in 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.
Sharing	**Toggle Panel**	Displays/hides the Workshare Connect panel in your Office window where you can see what's happening with a collaboration in real-time. Refer to *Monitoring shared files* for further information.
	Save to My Files	Enables you to save documents to Workshare online so they will be accessible to you online at all times. Refer to *Saving to My Files* for further information.
	Share	Enables you to share documents to groups in Workshare online so you can collaborate on them with others. Refer to *Sharing to a Workshare group* 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:
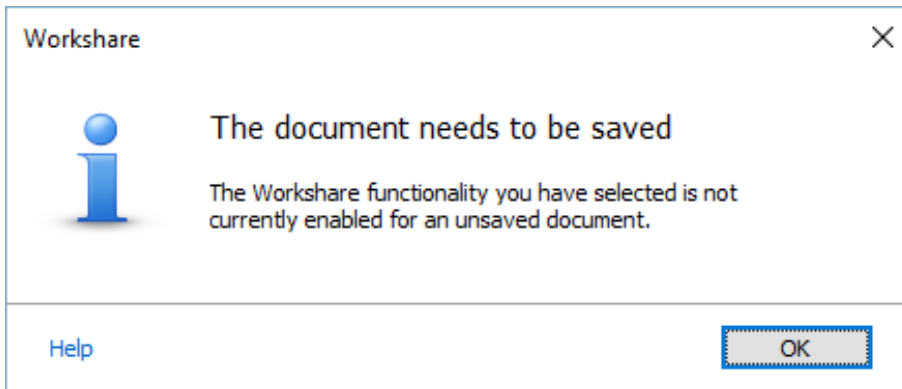
Licensing

After installation, you are prompted to log in to your Workshare account in order to retrieve your license entitlements. This can be in either of the following ways:
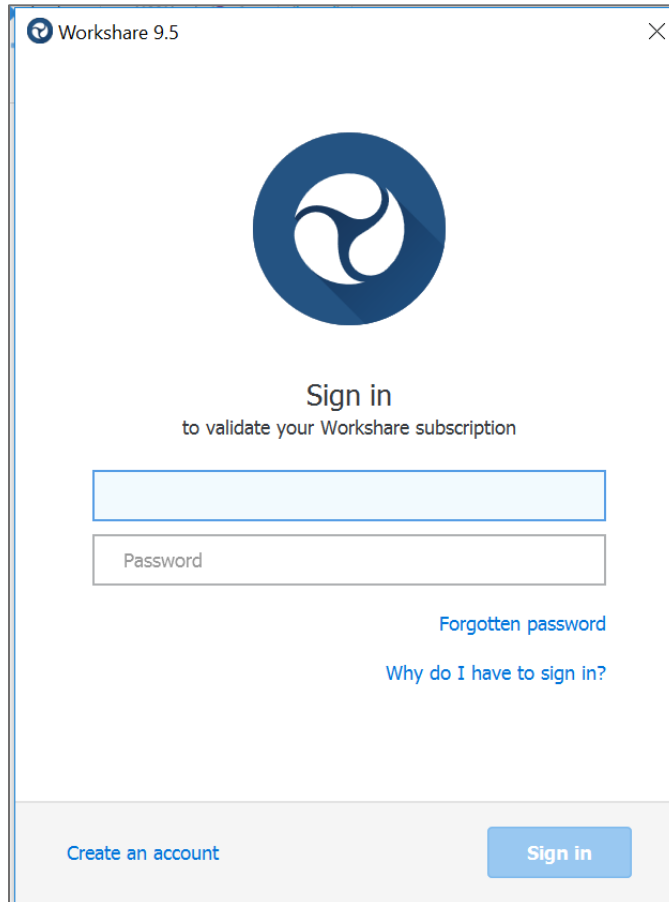
- When file share & sync is included in the installation, the Workshare desktop app is launched after install and you will see the following:
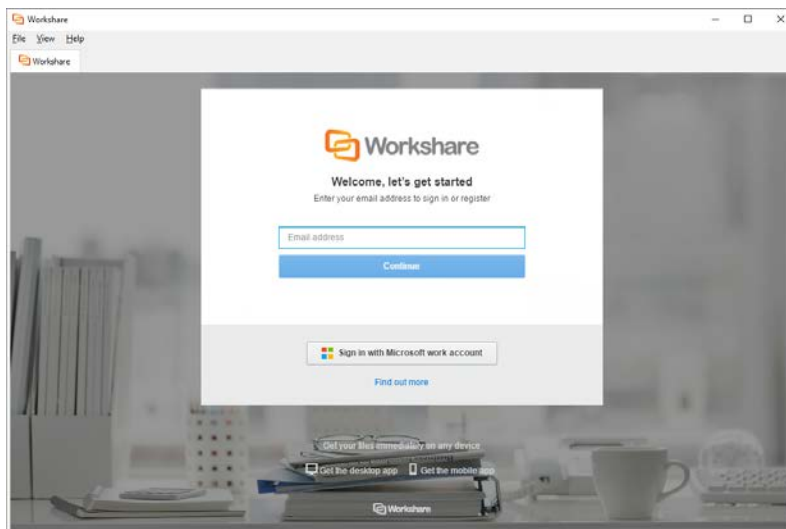
Enter your Workshare credentials (email address and password) and click **Sign in**. Your license entitlements are retrieved and you have access to all Workshare functionality. Your license entitlements are shown in the **My Products** tab of the Workshare Configuration Manager.

If you do not log in at this point, then…..

- The first time you access Workshare functionality, for example, by clicking any option in the Workshare tab, you will see the following:

> **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 16, 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 16, describes how to discover all content risk in Office documents.

- **Cleaning Hidden Data**, page 18, describes how to remove selected types of hidden data from a document and from multiple documents.

- **Converting to PDF**, page 24, 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 *Workshare* 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.
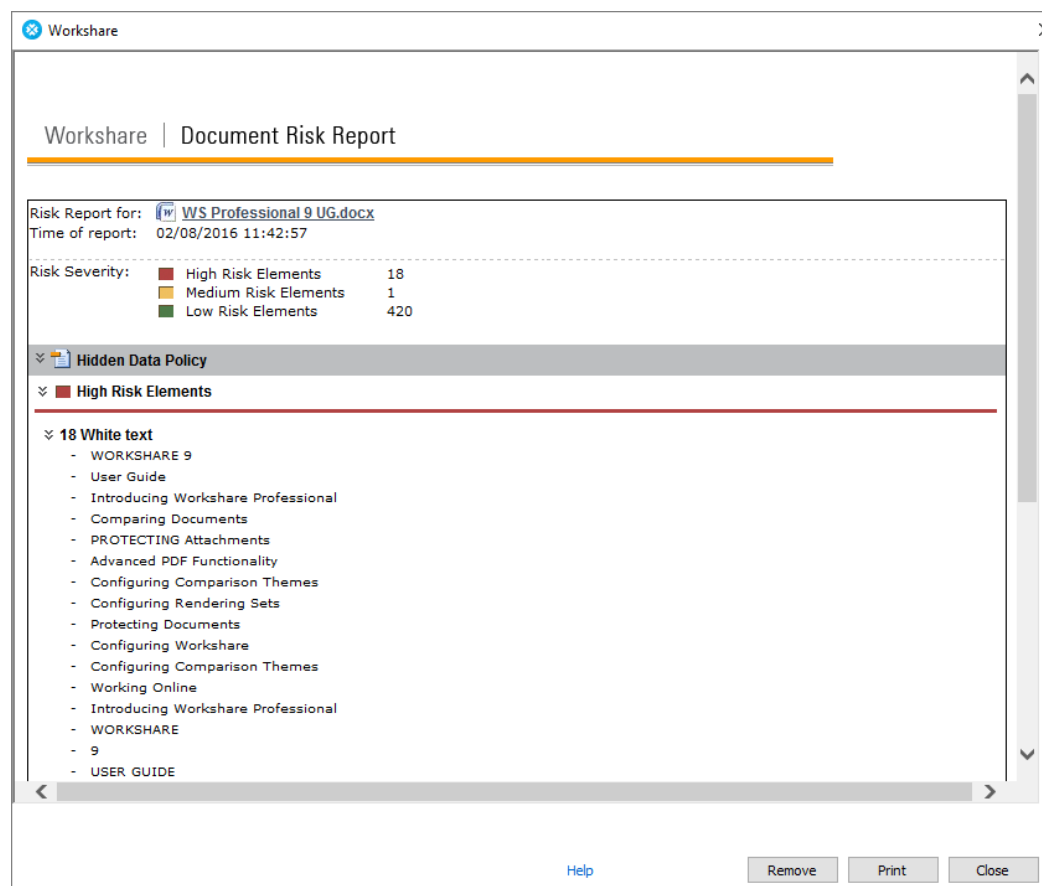
   The content risk found is divided into high risk, medium risk and low risk.

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.
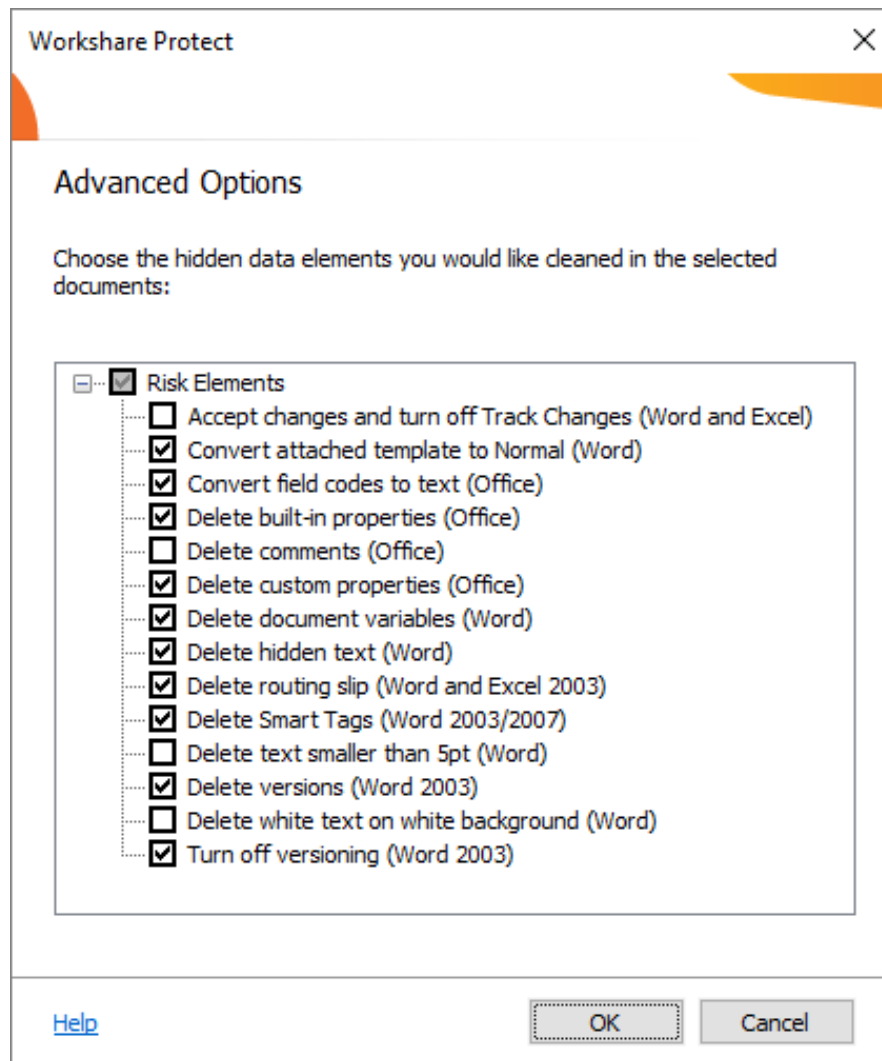
A complete list of hidden data that can be removed, reset or converted is listed in the dialog. Different options will appear according to the type of document – Word, Excel or PowerPoint. For a full description of the different options, refer to *Cleaning options*.

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 **All Programs**, **Workshare**, and then **Workshare Batch Clean**. The *Batch Clean* dialog is displayed.
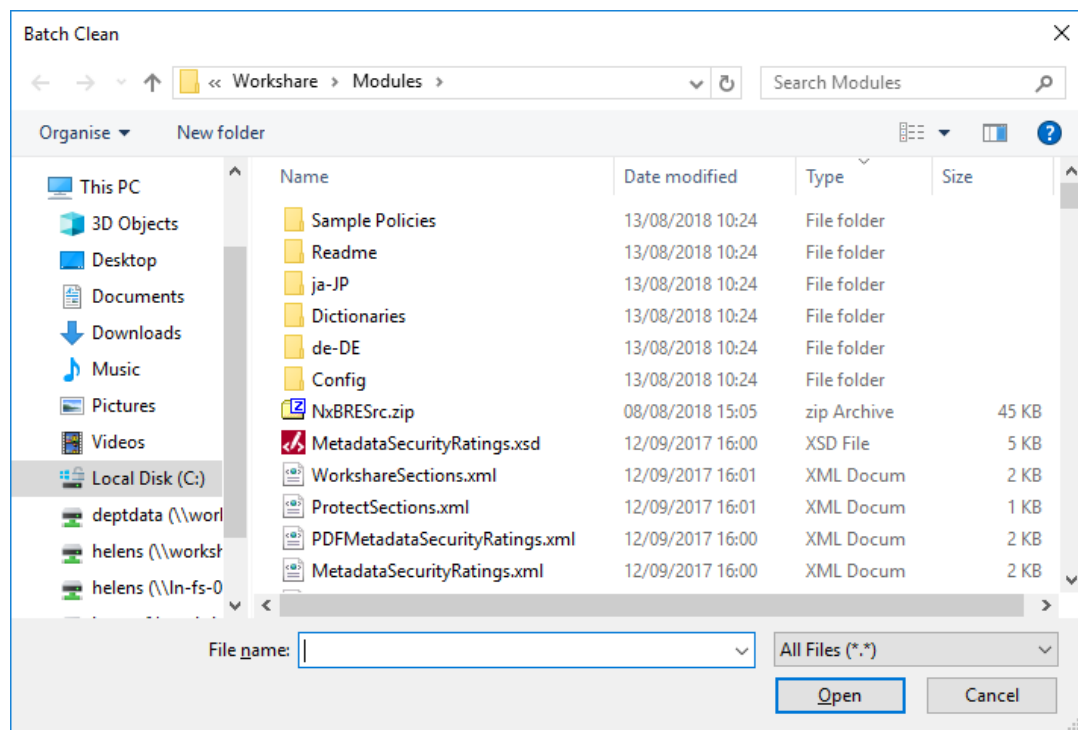
> *Note: To view more document types, select **All Office files** from the **Files of type** dropdown list. If unsupported file types are selected for batch cleaning, they will be ignored.*

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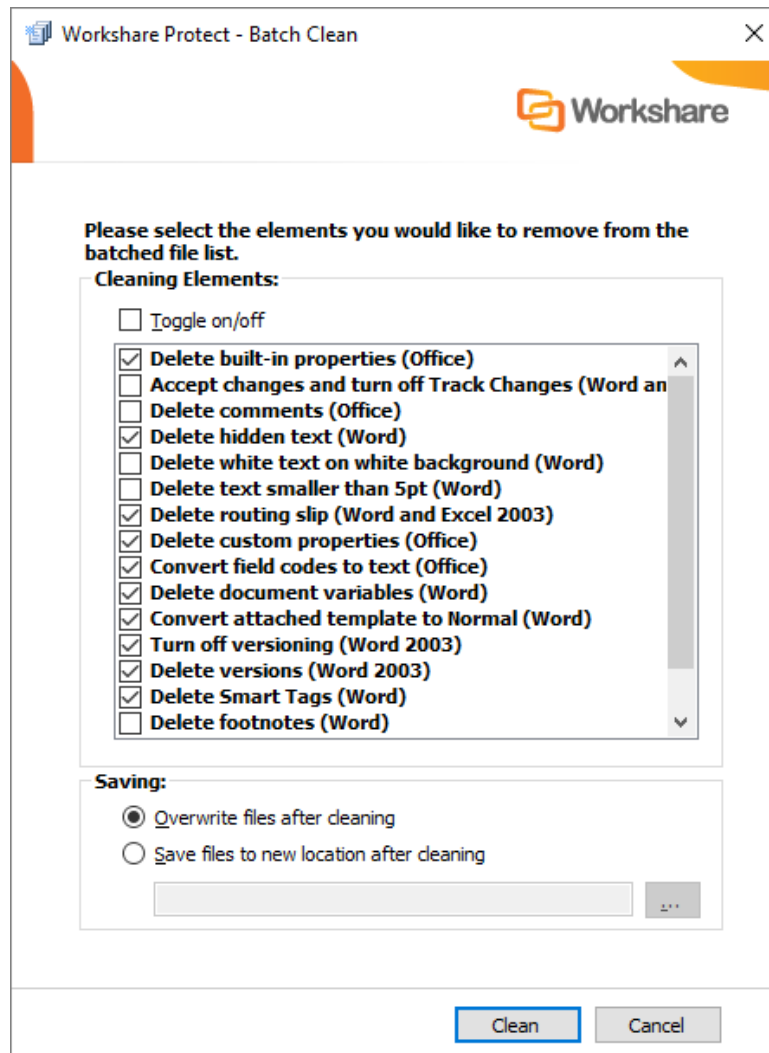
A complete list of hidden data that can be removed, reset or converted is listed in the dialog. For a full description of the different options, refer to *Cleaning options.*

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.
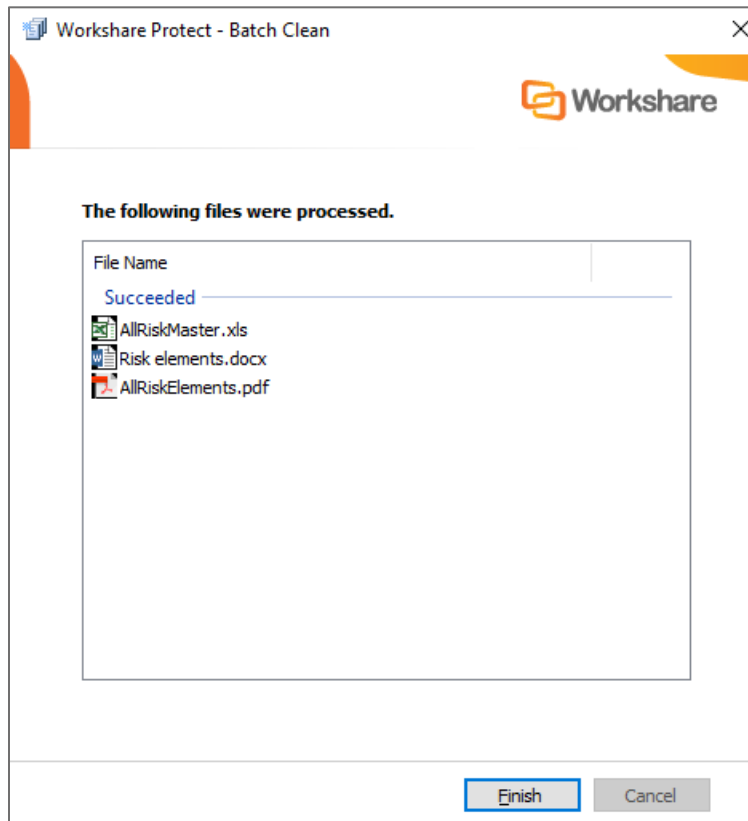
7. Click **Finish**.

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/
```


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.

Option	Description
`/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.

Option	Description
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.
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.

Option	Description
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.
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.

Option	Description
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.
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.

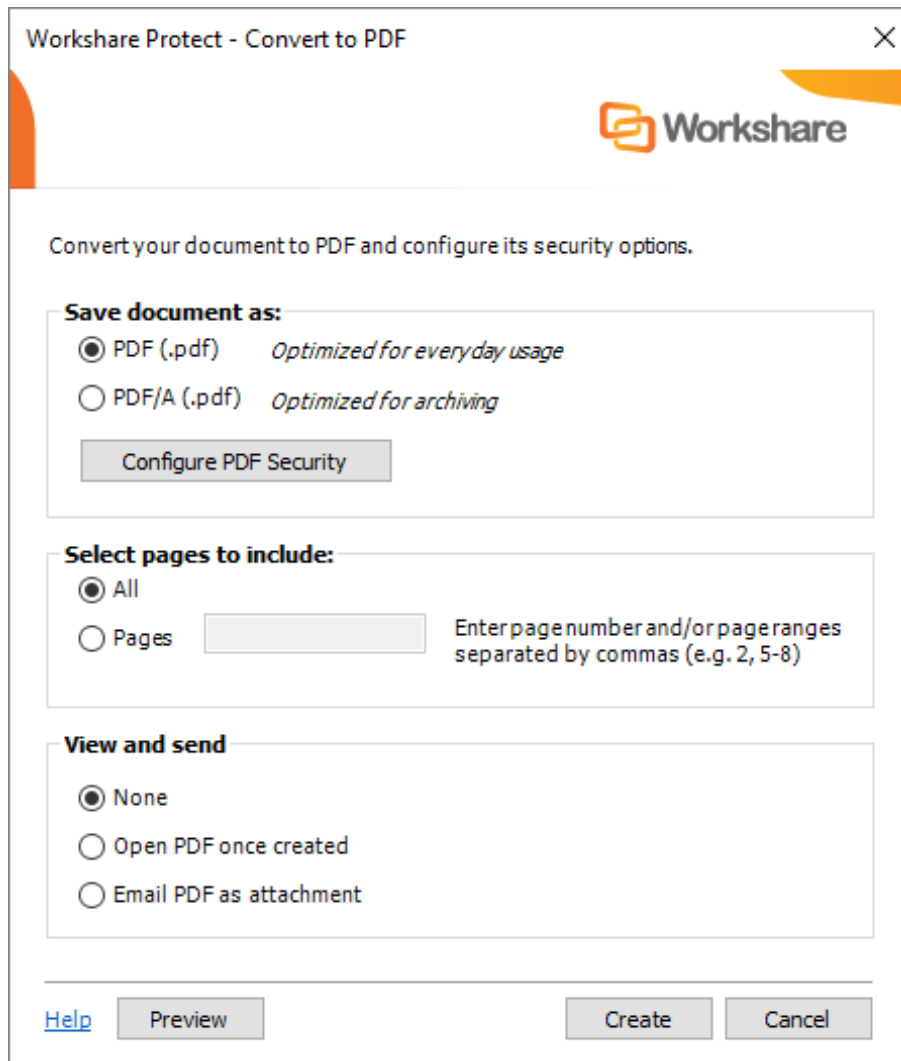| Option	Description
Turn off versioning (Word 2003)	Microsoft Word only. Turns off the flag to automatically save a new version of the document every time the document is closed. This applies to local file systems only. Versions can still be saved manually by saving a file with a different name.

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 Workshare 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.

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.

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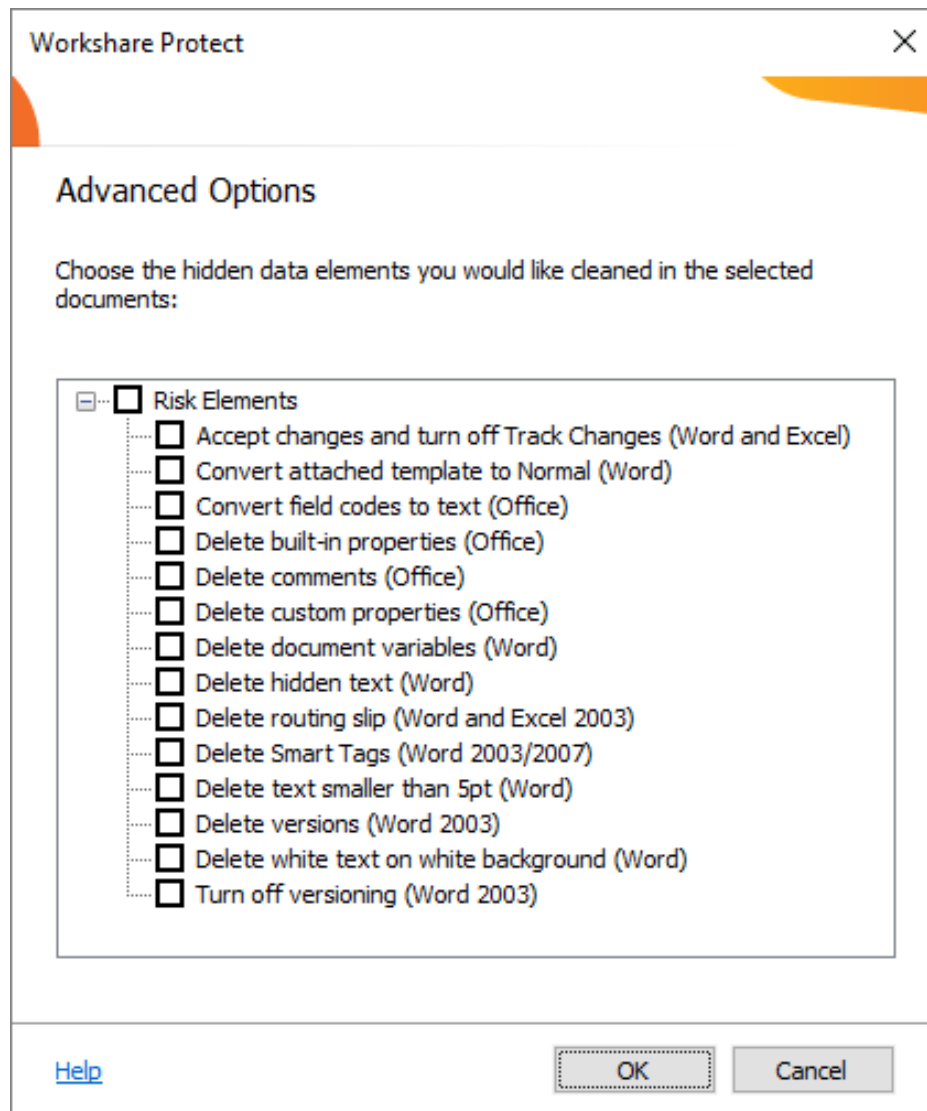
6. Select hidden data elements as required. For a full description of all the hidden data elements, refer to *Cleaning options* for further information.

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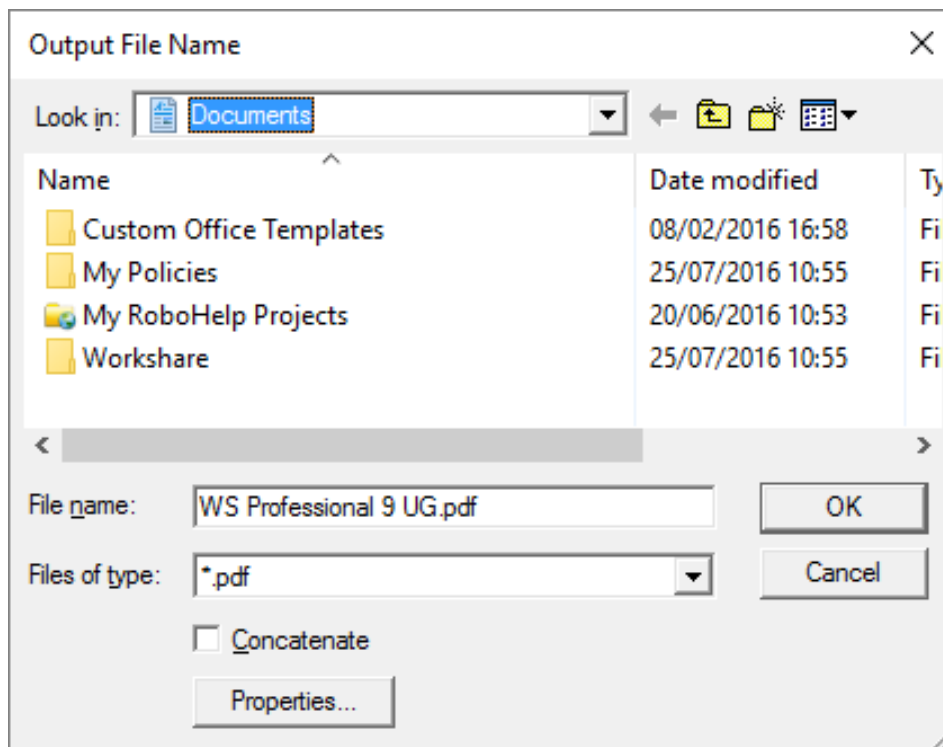
4. Specify a name for the PDF in the **File name** field or, if you want to add to an existing PDF, select the **Concatenate** checkbox and browse to and select the existing PDF.

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 34, introduces how Workshare Protect protects your files when sending by email.

- **Interactive Protect**, page 38, describes how to use Interactive Protect to secure your emails.

- **Using the Protect Profile Dialog**, page 48, describes how to send secure emails using the Workshare Protect Profile dialog.

- **Using the Email Security Dialog**, page 54, describes how to send secure emails using the Workshare Protect Email Security dialog.

- **Sending Links to your Files**, page 67, describes how to use the secure file transfer functionality to upload attachments to Workshare online and send recipients links to the files.

# Introducing Attachment Protection

> *Note: This chapter describes how to protect documents when emailing by removing metadata or converting to PDF or using secure file transfer. 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
- Send attachments to a secure location and send recipients a link to that location
- Compress multiple attachments into a single zip file

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

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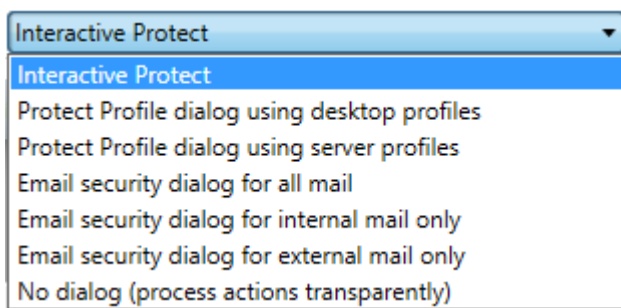
When sending emails, you may experience one of the following three options:

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

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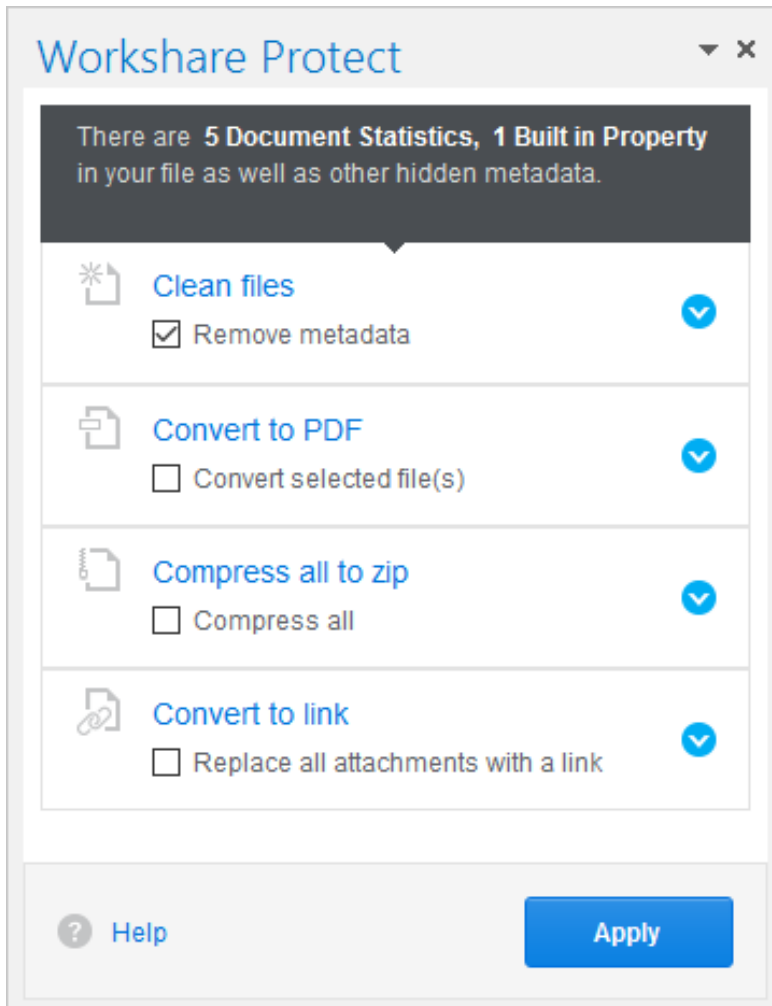
The Interactive Protect panel is displayed when **Interactive Protect** has been selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).

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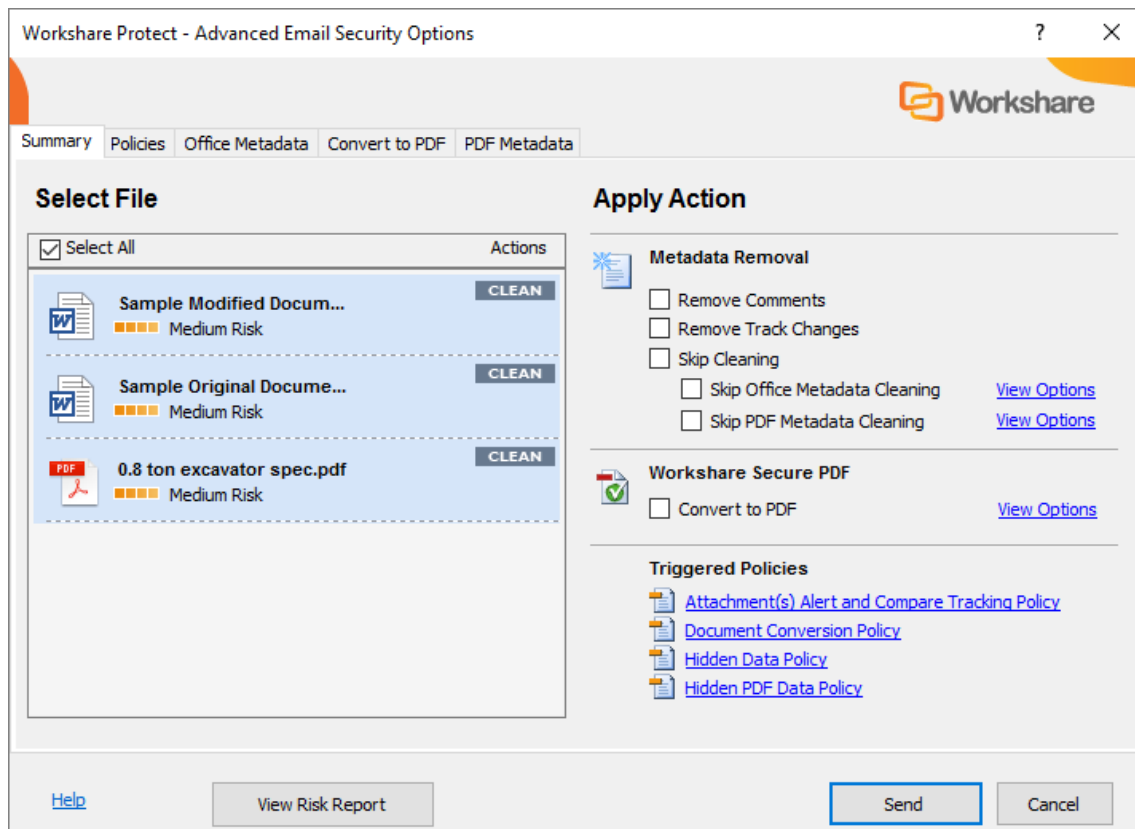
Protect Profile dialog
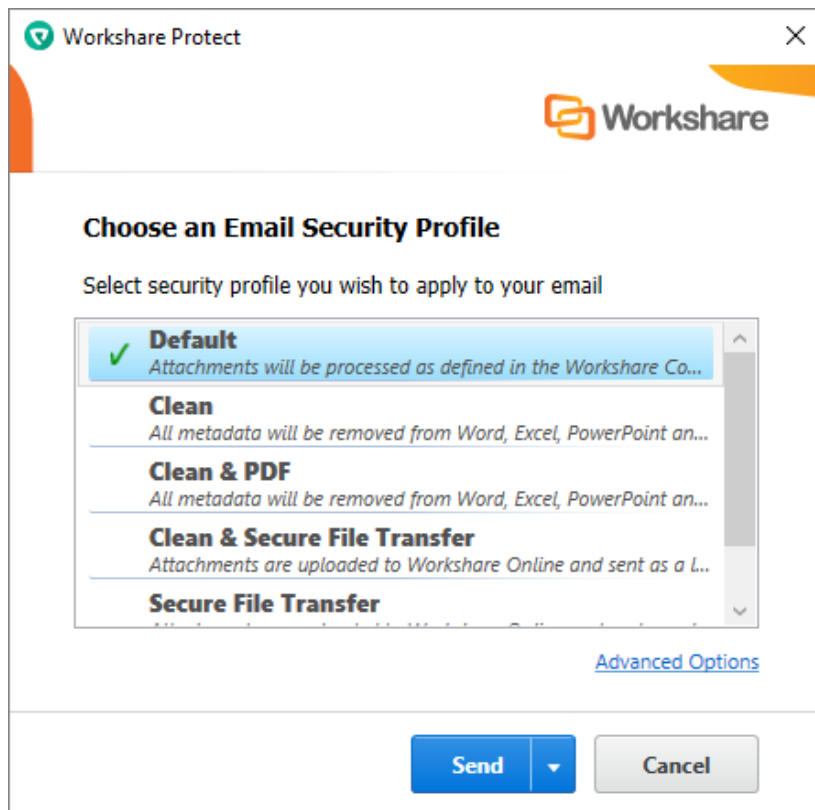
The Protect Profile dialog may be displayed in different ways depending on the option selected for the **After an email with attachments is sent show** parameter in the Workshare Configuration Manager (**Protection** > **Administration** category).

- **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

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.

- **Convert to link**: Enables you to send your documents to a secure folder in Workshare online and send recipients a link to that location.

To work with Interactive Protect:

Open Outlook and create a new email. Attach one or more files. Immediately Workshare Protect reports on the metadata found in a notification across the top of your email and the Interactive Protect panel on the right side of your email.
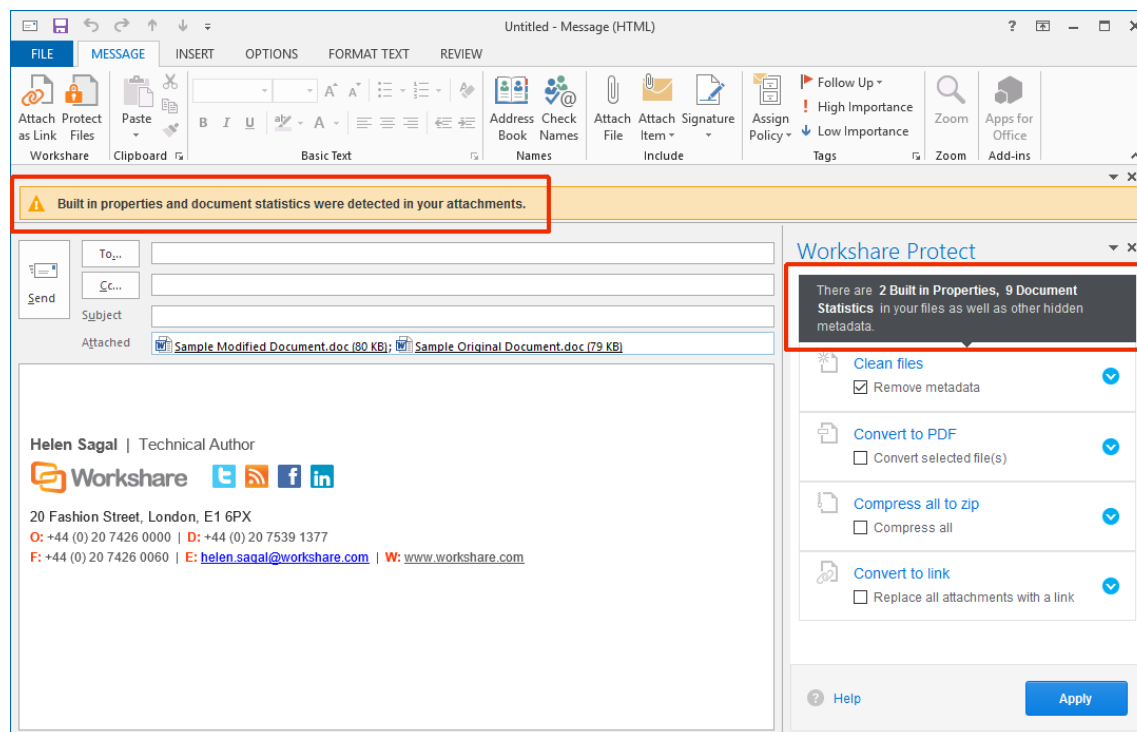
Note: *If the Interactive Protect panel doesn't open automatically, click the notification or click **Protect Files** in the Message tab.*

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. Additionally, you can send the attachments to a secure location in Workshare online and send a link to that location to the recipients.

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

If you do NOT click **Apply** before sending the email, 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.
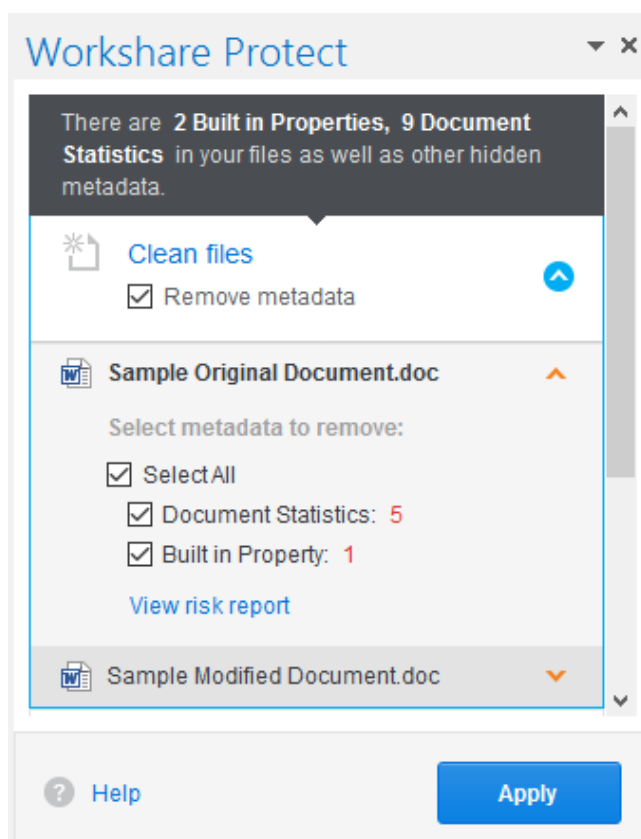
You can expand each attachment and adjust the metadata to remove for each one by selecting/deselecting the checkboxes.

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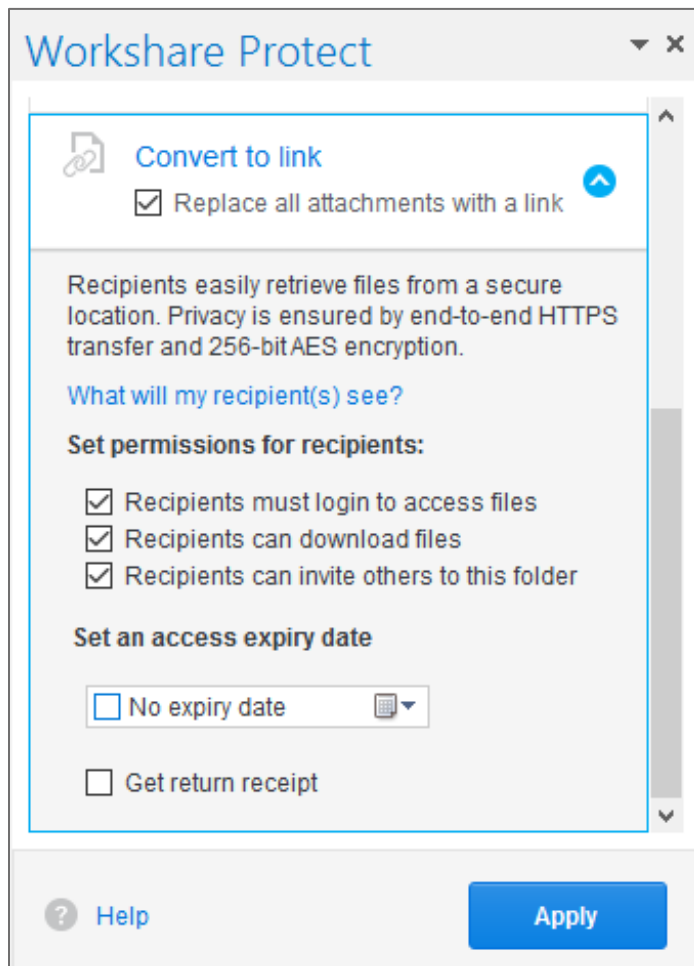
You can write your email while the attachments are being cleaned and then preview the files by opening the cleaned attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

Collaborating using Interactive Protect

When you work with Workshare online, you can send attachments to a secure location in Workshare. The attachment to your email is saved in a folder in your Workshare **Sent** folder in **Folders** and the recipient receives a link to the file.

To send a link to attachments:

1. In the Interactive Protect panel, select the **Replace all attachments with a link** checkbox.

2. To change the permissions set for the attachments in Workshare or to set an expiry date, expand the **Convert to link** section.

3. Deselect any of the following permissions for the attachments as required:

   ▫ **Recipients must login to access files**: When selected, the recipient must be a Workshare user and must log into Workshare in order to access the files.

   ▫ **Recipients can download files**: When selected, recipients can download the files.

   ▫ **Recipients can invite others to this folder**: When selected, recipients can share the folder where the attachments are stored.

4. If required, select an expiry date for the files. After this date, recipients will no longer be able to access the files.

5. Select the **Get return receipt** checkbox if you want to receive an email once the recipients have accessed the files.

6. Click **Apply**. You can write your email while the attachments are being processed and then preview the files in Workshare online by clicking the link.

> *Tip! You can clean, convert to PDF or compress the attachments before uploading to Workshare online using options in the Interactive Protect panel.*
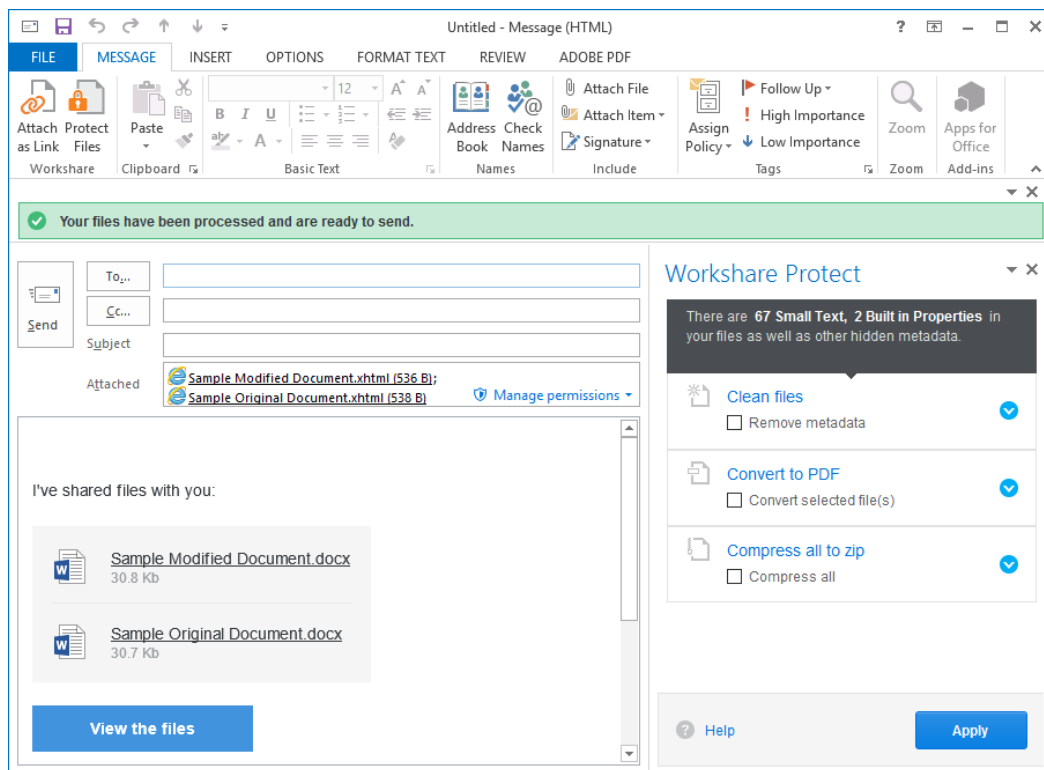

If required, click **Manage Permissions** in the attachments bar and change the permissions set for your files.

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

The attachments are uploaded into a single folder in your **Sent** folder in Workshare online and in the recipients' **Received** folder. The name of the folder is whatever you entered in the **Subject** field.

The folder is created as soon as the attachments are converted to links and if you look in Workshare before you click Send, you will see the folder and the names of the files with upload pending.
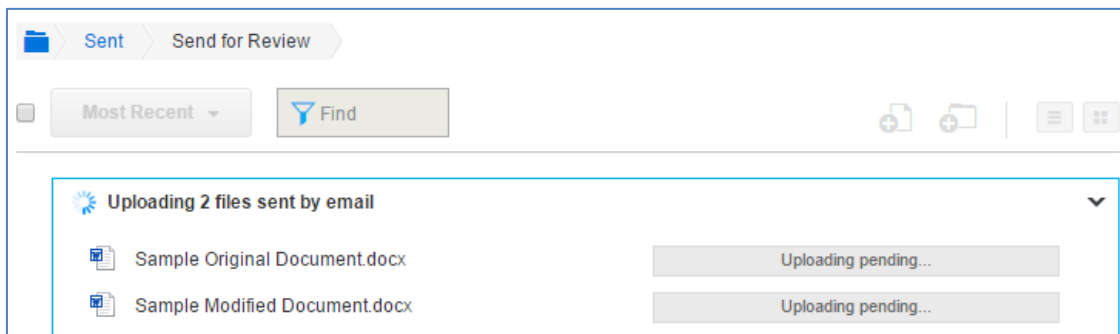
Once your email is sent, the files are uploaded to Workshare. The recipients will receive your email straightaway and they can click the link to view the files in Workshare. If the files are still uploading, upload pending is displayed.

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.

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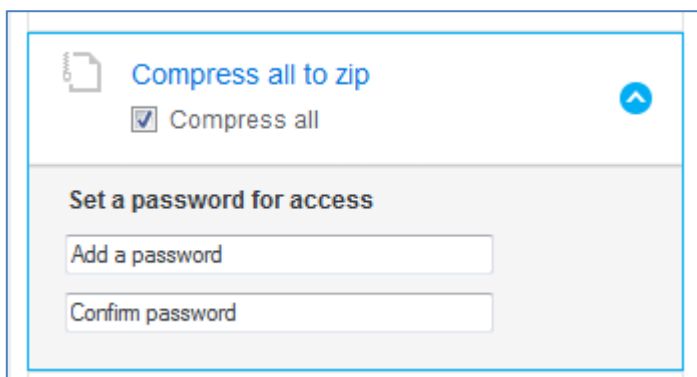
You can write your email while the attachments are being converted and then preview the files by opening the converted attachments. Finally click **Send** once you are confident that what you are sending is secure and safe.

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 and then upload the zip file to Workshare online.*

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


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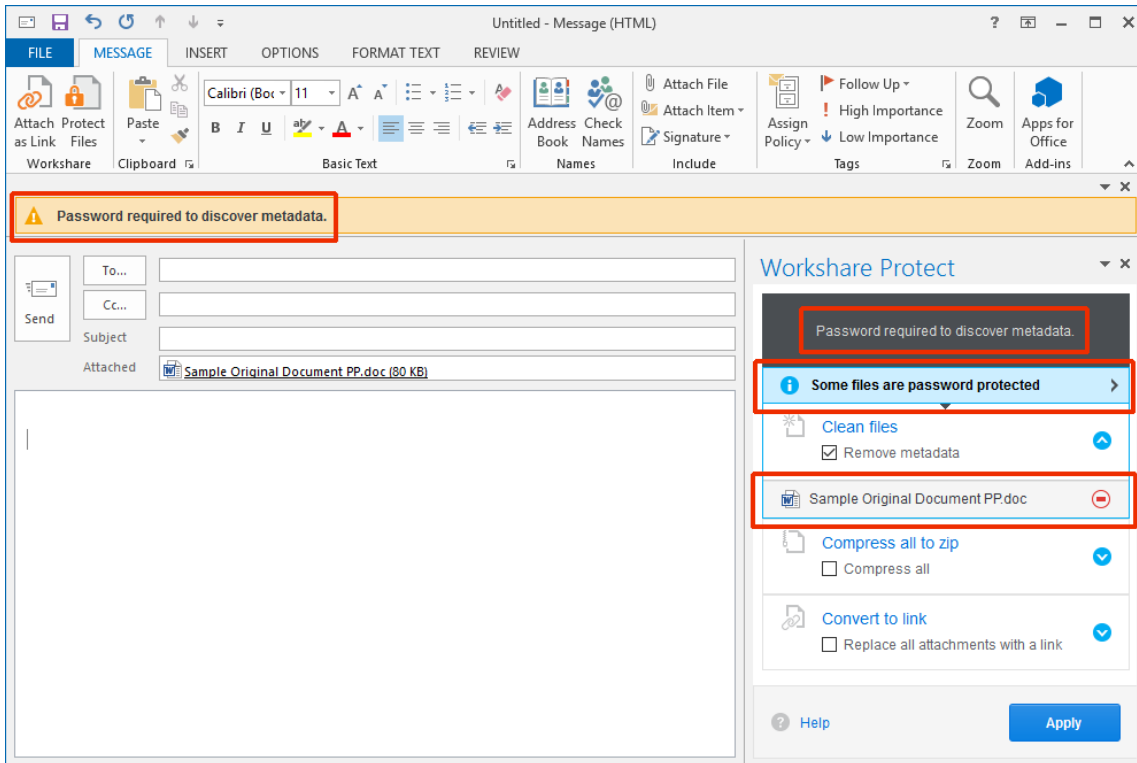
In order to proceed and clean the attachment or convert it to PDF, you must enter the open/modify password.

Click the ⊖ icon. The *Password required* dialog is displayed.
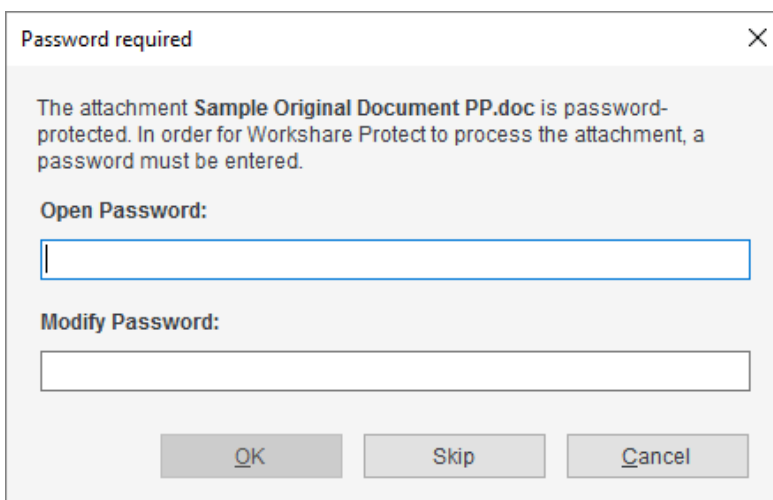
Enter the open or modify passwords (or both) and click **OK**.

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

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

Using the Protect Profile Dialog

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

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

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

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

- **Task-based profiles**: For example, you are working on a legal document and sending it to colleagues to receive input. You email it and select the "Working Draft" profile which will remove metadata but keep track changes and comments. After receiving input and implementing changes, you email it and select the "Final Draft" profile which will remove metadata and remove track changes and comments. Once you are happy with the document, you email it and select the "Final" profile which will remove metadata, track changes and comments and convert the document to PDF.

- **Recipient-based profiles**: For example, your company has a policy that whatever documents you send to opposing counsel, the metadata must be removed and the document must be converted to PDF. You therefore have a profile called "opposing counsel" which removes metadata and converts to PDF. You also have a profile called "Personal" which does nothing.

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

To send an email:

1. Create a new email, attach the required document(s) and click **Send**. The *Protect Profile* dialog is displayed.
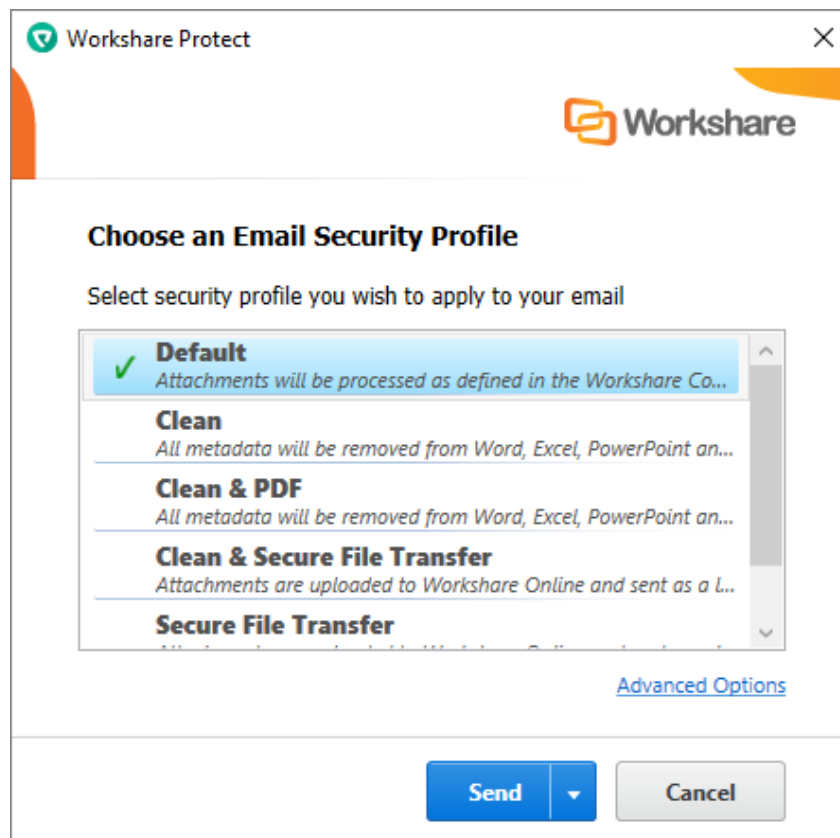
2. Select the profile you want to apply to your attachments and click **Send**. The following profiles are provided with Workshare Protect:

   - **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.
   - **Clean & Secure File Transfer**: All metadata is cleaned from Microsoft Word, Excel, PowerPoint and PDF attachments and then the attachments are uploaded to Workshare online and recipients are sent a link to the attachments. Refer to *Secure File Transfer Profiles*, page 50.
   - **Secure File Transfer**: Attachments are uploaded to Workshare online and recipients are sent a link to the attachments. Refer to *Secure File Transfer Profiles*, page 50.

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.

Secure file transfer profiles

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

To securely transfer files:

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

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

3. Select **Secure File Transfer** or **Clean & Secure File Transfer** (if you want to remove metadata from the attachments before uploading them to Workshare online).
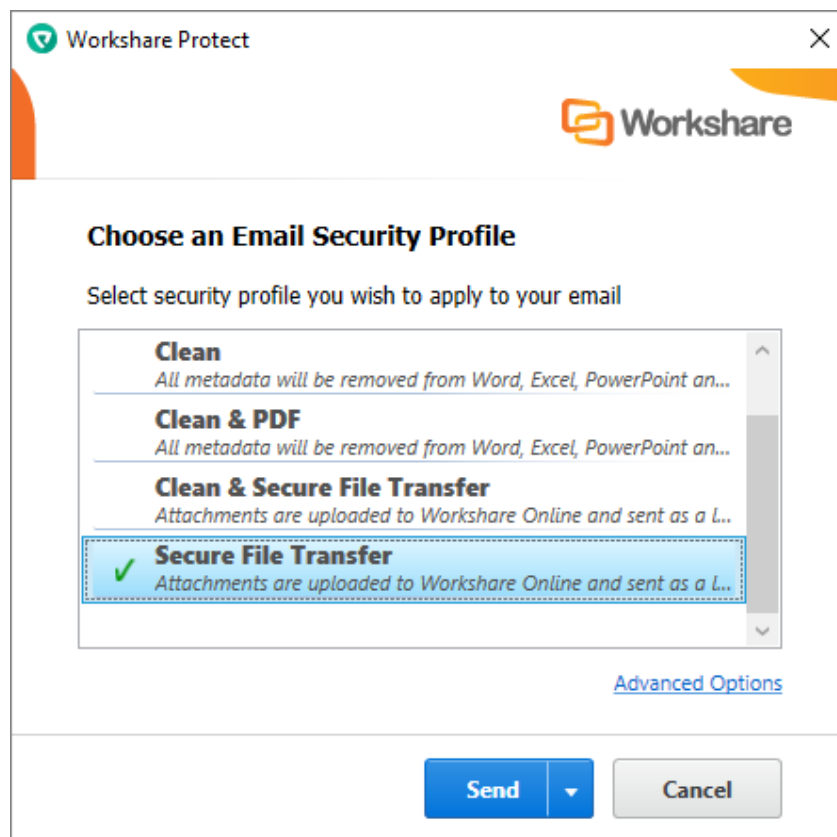
> *Note: Click **Advanced Options** if you want to configure specific user access to the documents in Workshare. Refer to Setting advanced options.*

4. Click **Send**. The attached files are uploaded into a single folder in your **Sent** folder and the recipients **Received** folder (in **Folders** in Workshare online). The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time.

Setting advanced options

If your administrator has given you the rights to access the advanced options, you can set access rights to documents that you upload to Workshare online to control recipient access. Clicking **Advanced Options** in the *Protect Profile* dialog enables you to configure specific user access to the documents you are uploading to Workshare online.

To configure advanced options:

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

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

3. Select **Secure File Transfer** or **Clean & Secure File Transfer** and click **Advanced Options**. The *Advanced Email Security Options* dialog is displayed.

4. Select the **Secure File Transfer Action** tab.
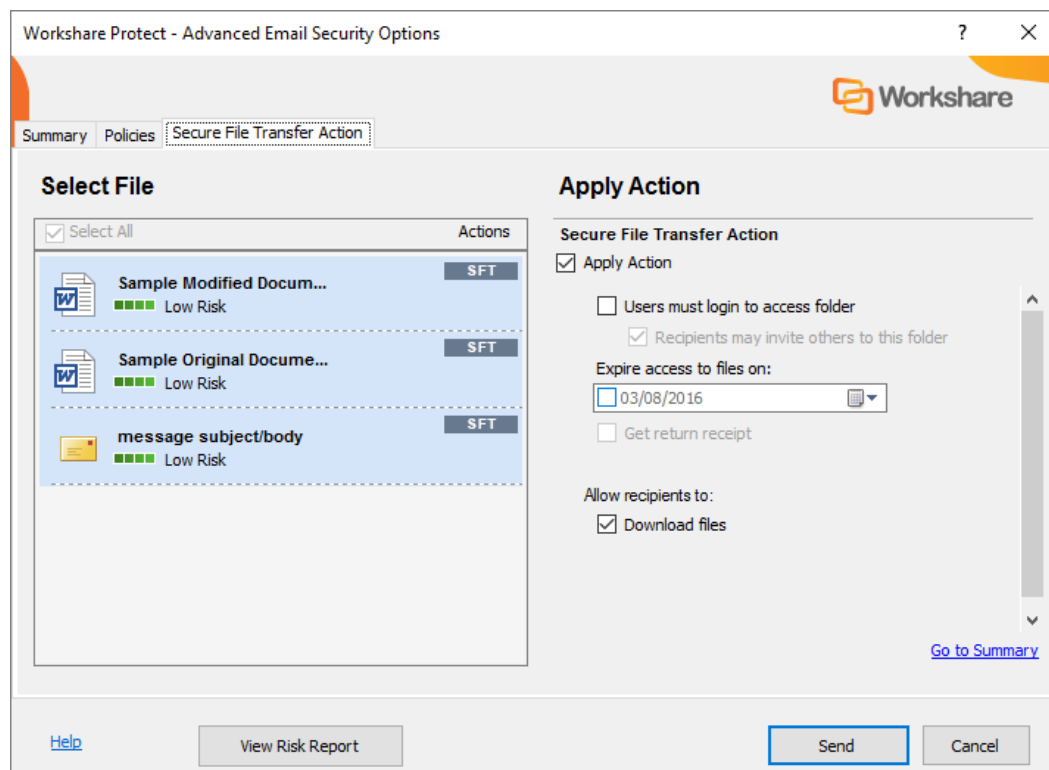
5. You can configure the following parameters:

Apply Action	When selected the selected profile (**Secure File Transfer** or **Clean & Secure File Transfer**) is applied to the email. When not selected, the email is sent without a profile being applied.
Users must login to access folder	When selected, the recipient must log into Workshare in order to access the file. When not selected, the recipient can access Workshare without being a registered user to view and download the file only.
Recipients may invite others to this folder	When selected, recipients can forward the link to other recipients who will be able to access the file. Unless **Users must login to access folder** is selected, this option is always selected.
Expire access to files on:	You can specify an expiry date for the file. After this date, the recipient will no longer be able to access the file.
Get return receipt	When selected, you will receive an email once the recipient has accessed the file.
Download files	When selected, recipients can download the file.

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

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

7. Click **Send**. The attached files are uploaded into a single folder in your **Sent** folder and the recipients **Received** folder (in **Folders** in Workshare online). The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time.

Receiving links to files in Workshare online

Recipients of emails sent using secure file transfer from the *Protect Profile* dialog receive an email with details of the name of the file and a link to click to access the file in Workshare online. The means of access and options available to the recipient will vary depending on whether the recipient is a Workshare user and the settings specified by the sender. Scenarios include:

- When a recipient is a Workshare user, clicking the link displays the location in Workshare online where the file (or files) is stored. The file or files are stored in a folder with a name that matches the subject of the email. This folder appears in the recipient's **Received** folder (in **Folders** in Workshare online). The recipient can add comments to the file, upload versions and make changes to the folder where the file is stored.

- If the sender has specified that the recipient need not be a Workshare user, clicking the link displays the location in Workshare online where the file (or files) is stored. The recipient can view the file and download it.

- If the sender has specified that the recipient must be logged in to Workshare, clicking the link displays the Workshare login and the recipient must first log in to Workshare in order to view the file (or files) and download it.

- If the sender has specified an expiry date then the link will only work until the expiry date. Once the date has passed, the recipient will not be able to access the file.

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.
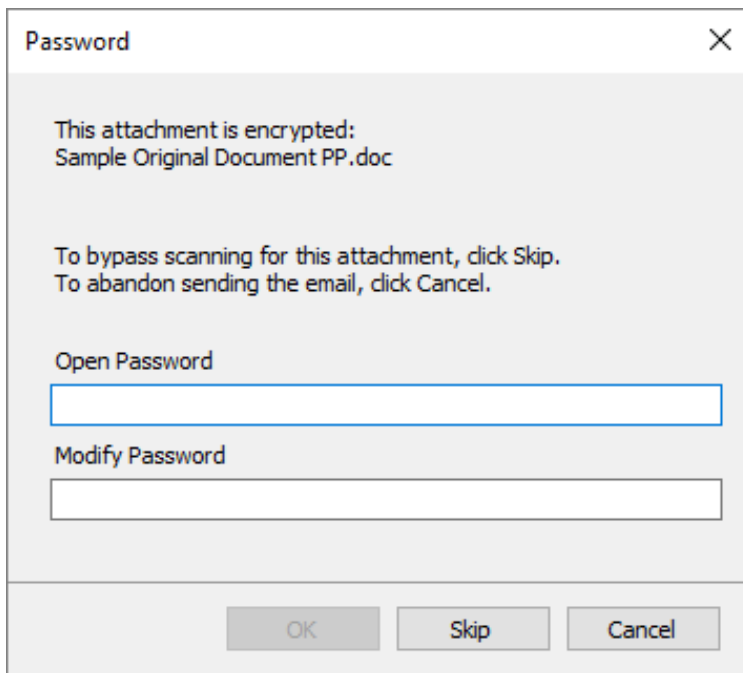
*Note: Workshare Protect will only check attachments of emails sent internally or externally (or both) if Workshare Protect is turned on for internal or external emails (or both). This is done using the **Apply Workshare Protect** parameter in the Workshare Configuration Manager (**Protection** > **Administration** 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,
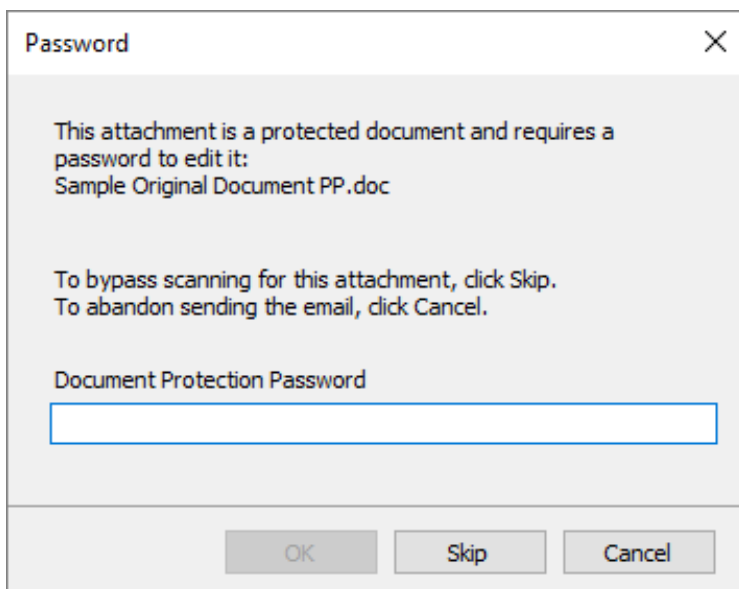

Enter the password required to open the document in the **Open Password** or **Modify Password** field and click **OK**, or you can click **Skip** and Workshare Protect will not check the document.

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,

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.
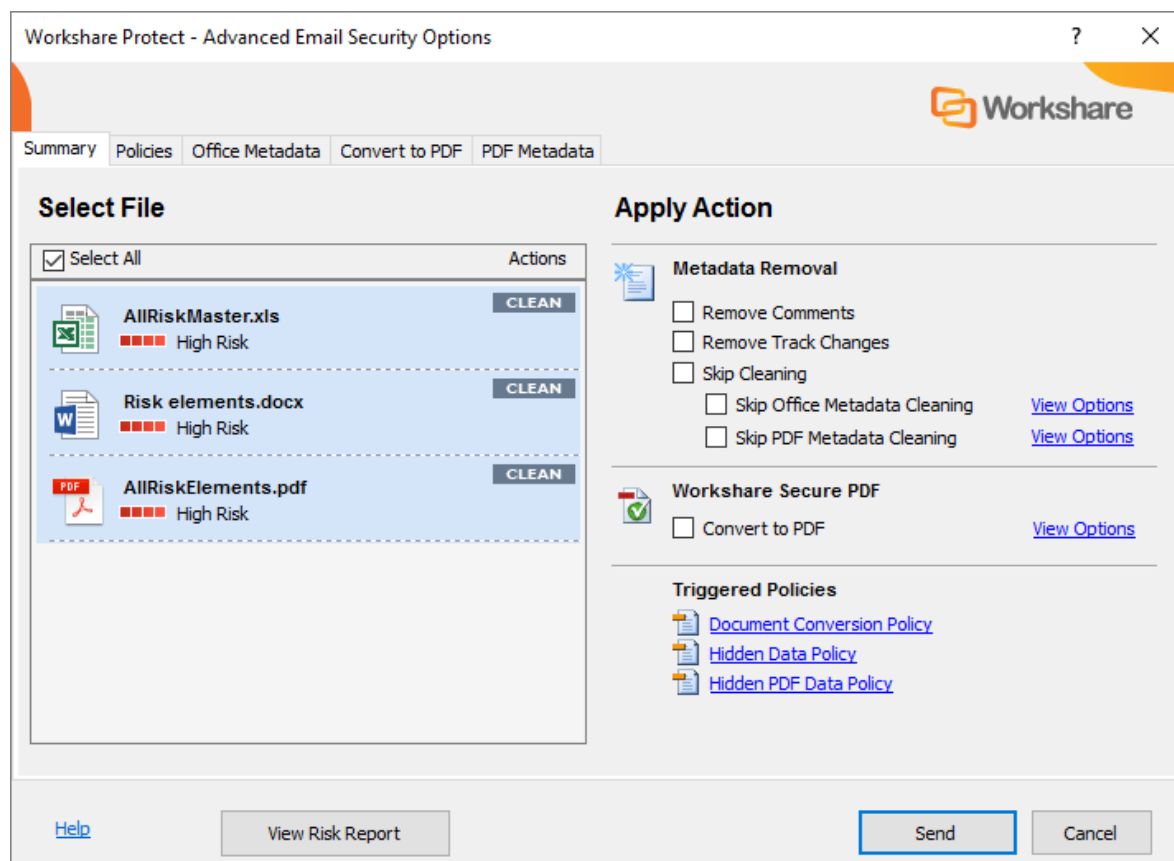
This dialog alerts you to any breaches of security policies in the default profile triggered by your email or its attachments. If your administrator has given you permissions, you can modify the settings for each attachment. Refer to *Quick tour of the Email Security dialog* for further information about 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.
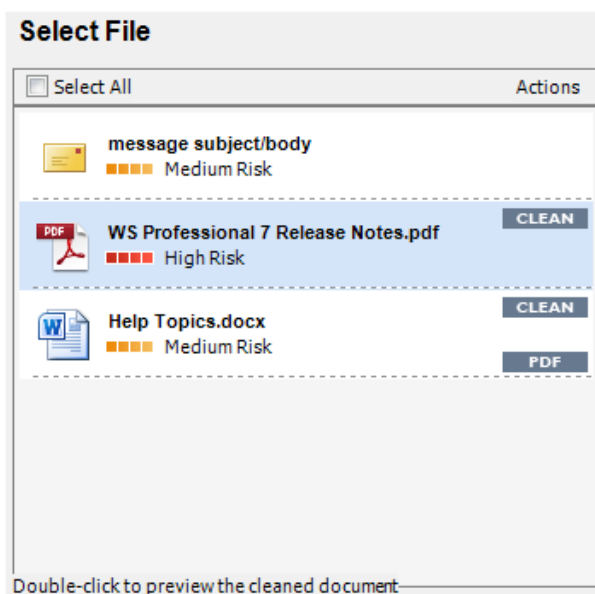
For each item, you can see the risk level and the actions to be applied to the item. You can select individual attachments or select the entire list by selecting the **Select All** checkbox. When a Clean or PDF action is to be applied, you can double-click an item in the list to preview what it will 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.

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.

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.

The **Secure File Transfer Action** tab is included in the *Email Security* dialog when a Secure File Transfer profile is selected in the *Protect Profile* dialog. Refer to *Secure file transfer profiles.*

Resolving blocked emails

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

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

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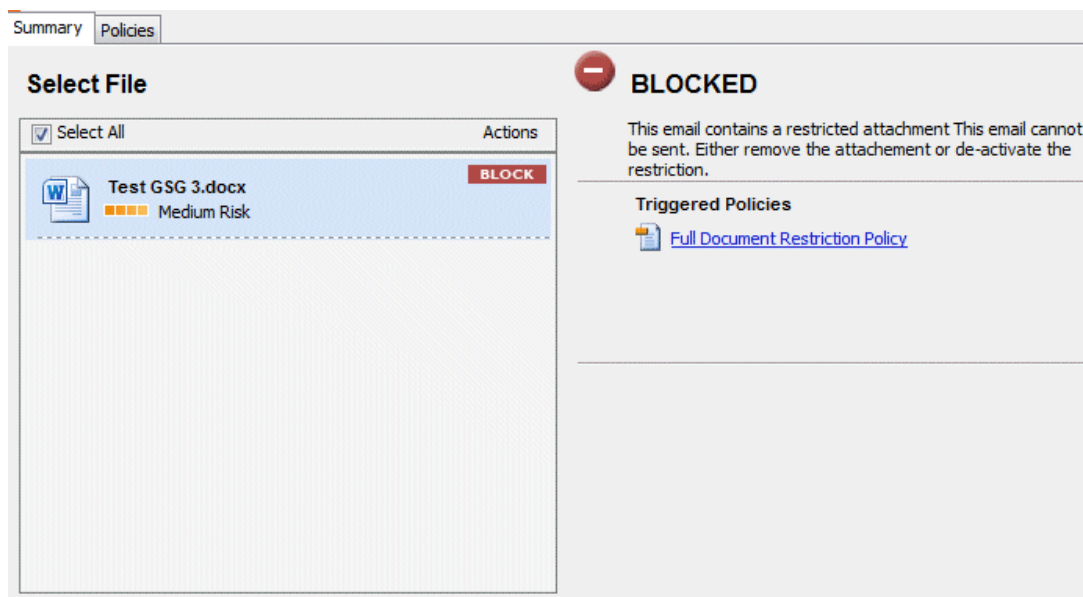
To resolve blocked emails:

1. Click the name of the policy in the **Triggered Policies** list or select the **Policies** tab to view what content has triggered the email policy.

2. Click the **Close** button to close the *Email Security* dialog.

3. Make the appropriate changes to the email and/or document(s) by removing or modifying the content, attachments or recipients that caused your email to be blocked.

4. If making changes to attachments, re-attach the corrected documents.

5. Click **Send**. If you have made all the relevant changes, you should now be able to send the email successfully.

Reviewing alerts

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

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

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

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

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

Cleaning hidden data from attachments

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

Your system administrator can define policies that contain certain pre-defined policy triggers that oblige you to clean hidden data from attached documents when they are sent by email. The **Clean**, **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.


> **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.
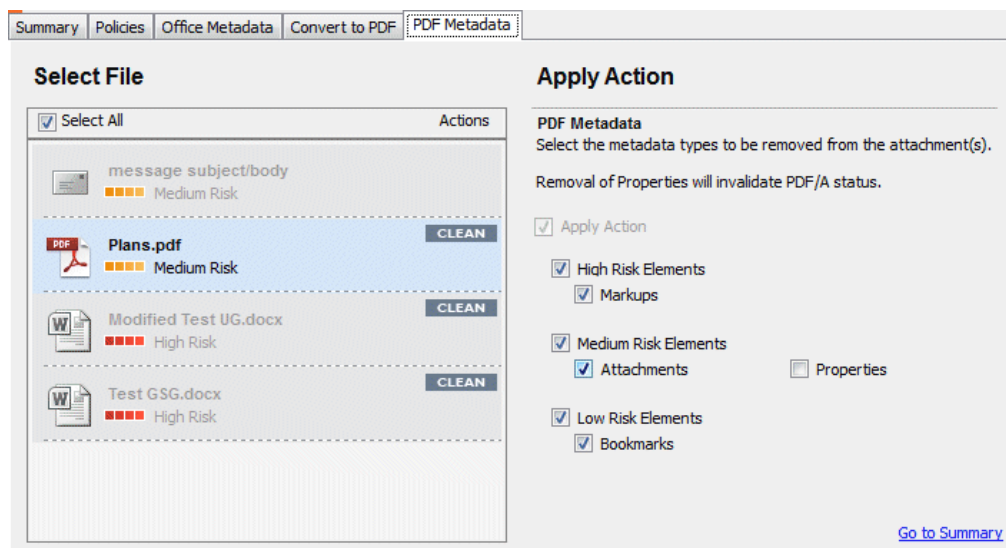
To clean hidden data:

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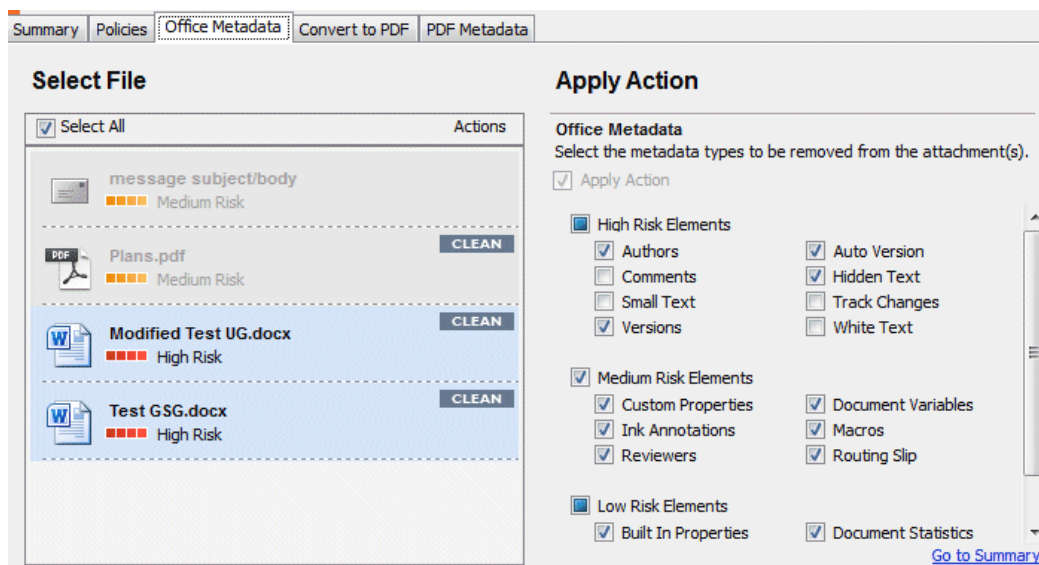
3. Select the hidden data that you want to remove by selecting or deselecting the relevant checkboxes.

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.

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.

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.

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

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

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

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

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

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

5. Select the **PDF/A** checkbox to convert the attachment to PDF/A.

6. Repeat steps 2 to 5 for additional attachments if required.

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

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

Sending Links to your Files

Your administrator may have configured Protect to automatically convert your attachments to links according to attachment size or using a shortcut in the attachments bar.

Links shortcut

Whatever the Protect user experience set up in your environment, when you have a shortcut on the attachment bar, you can convert your attachments to links in a single click.

The configuration required for this option is in the Workshare Configuration Manager as follows:

Category	Parameter	Default
Protection > Sharing	Display Link on attachments bar	Not selected

Whenever you add attachments to an email, the **Link** option is displayed in the attachments bar.
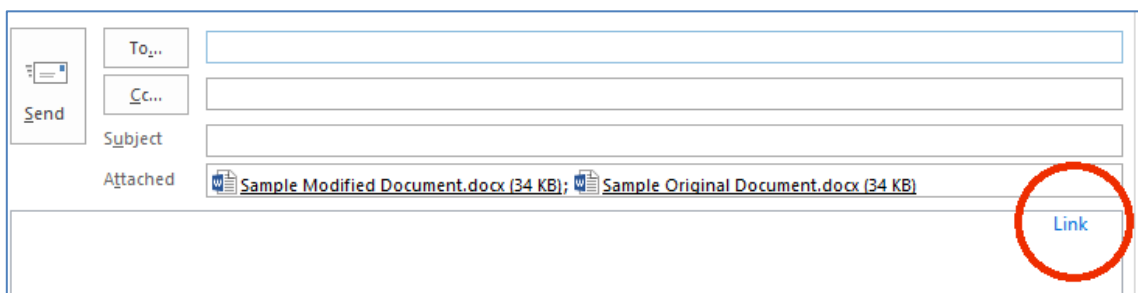
Click **Link** and your attachments are converted to links and appear in the body of your email.
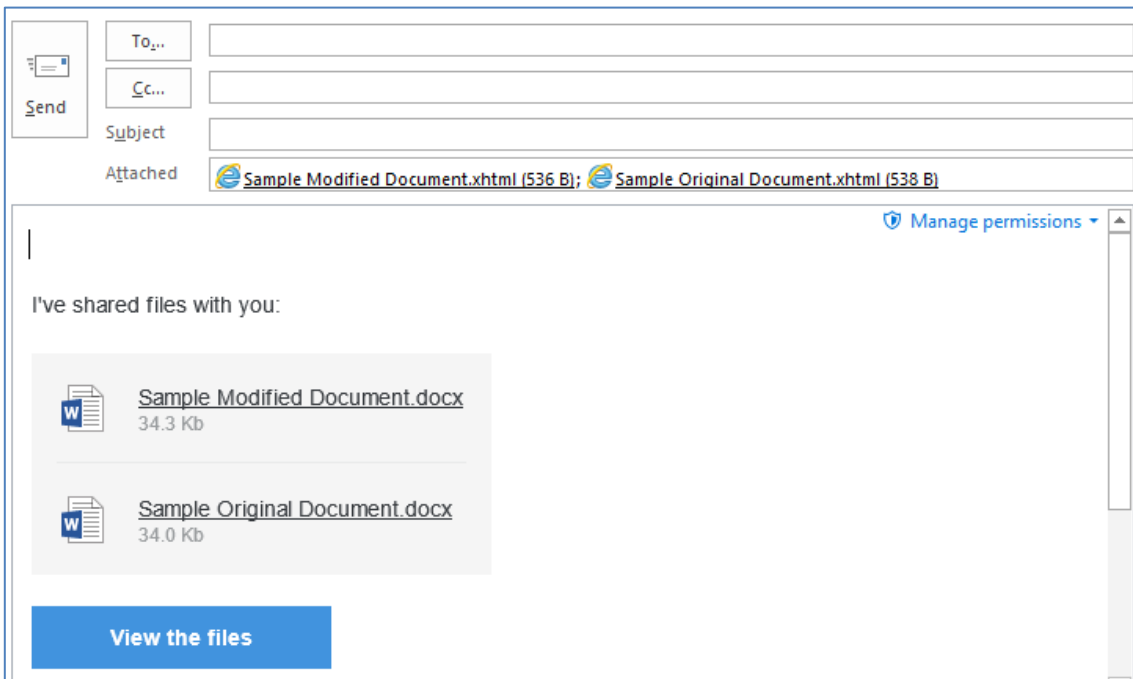
> **Note**: If required, click **Manage Permissions** in the attachments bar and change the permissions set for your files, such as whether recipients can download the files.

The attachments are uploaded into a single folder in your **Sent** folder in Workshare and in the recipients' **Received** folder. The name of the folder is whatever you enter in the **Subject** field.

The folder is created as soon as the attachments are converted to links and if you look in Workshare before you click **Send**, you will see the folder and the names of the files with upload pending.
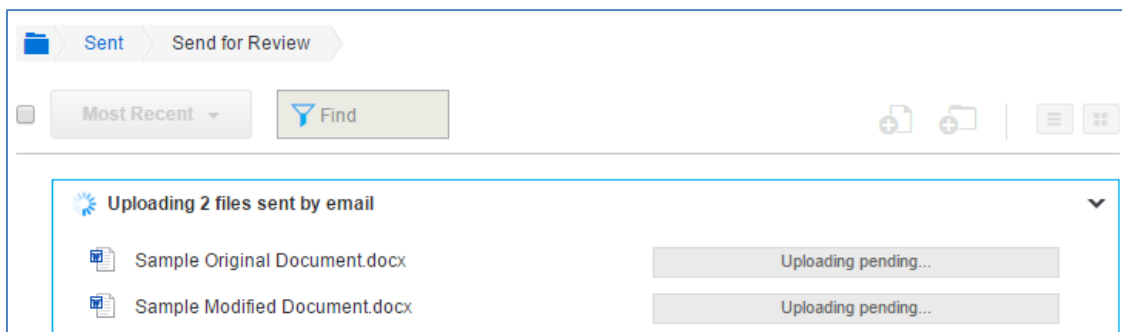
Once your email is sent, the files are uploaded to Workshare. The recipients will receive your email straightaway and they can click the file names or the **View the files** button to view the files in Workshare. If the files are still uploading, upload pending is displayed.

Large attachments

In order to avoid blocking email with large heavy files, you can upload the files to Workshare and send recipients a link to those files. There are several ways this can be done depending on your configuration.

Auto convert

The configuration required for this option is in the Workshare Configuration Manager as follows:

Category	Parameter	Default
Protection > Sharing	Automatically convert to link(s) when total attachment size exceeds (MB)	No size specified

If a limit has been set for this parameter, as soon as you attach files above this limit, they are automatically converted to links.

The links appear in the body of your email and the attachments are uploaded into a folder in Workshare.

Attach as Link button

The configuration required for this option is in the Workshare Configuration Manager as follows:

Category	Parameter	Default
Protection > Sharing	Display Attach as Link button (Outlook)	Selected

When auto convert is not set up and your administrator has set a limit on attachment size (to avoid large files blocking Exchange), when you try and add a file with a size over the specified limit, Microsoft Outlook displays a message such as:
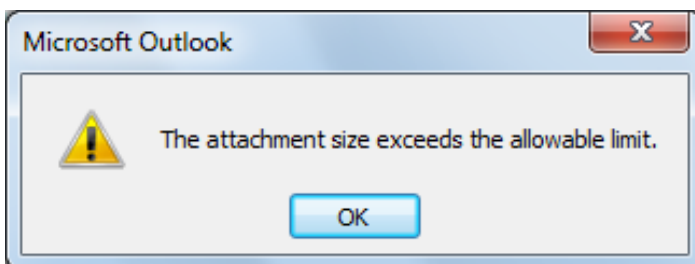
In this case, you can use the **Attach as Link** button to save the large file to a folder in Workshare and send recipients a link to the location.

The procedure will vary depending on the Protect user experience set up.

When Interactive Protect is configured:

1. Click **Attach as Link**.

2. Browse to the file you want to send.

3. Click **Open**. A link to the file appears in the body of your email.

4. Repeat steps 1 to 3 to add further files.

Once your email is sent, the files are uploaded to Workshare. The recipients will receive your email straightaway and they can click the file names or the **View the files** button to view the files in Workshare. If the files are still uploading, upload pending is displayed.

When the Protect Profile dialog is configured:

1. Click **Attach as Link**.

2. Browse to the large file you want to send and click **Open**.

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

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

The large file is uploaded to a folder in your **Sent** folder (in **Folders**) in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email. The recipient receives an email notifying them that file has been uploaded to Workshare online and providing a link to the file.

Auto select Convert to Link

The configuration required for this option is in the Workshare Configuration Manager as follows:

Category	Parameter	Default
Protection > Interactive Protect	Automatically select 'Convert to link' when total attachment size exceeds (MB)	No size specified

If a limit has been set for this parameter and you have Interactive Protect configured, when you attach a file over the specified limit, the **Replace all attachments with a link** checkbox in the **Convert to link** area is selected when the Interactive Panel displays. Simply click **Apply**, complete your email and click **Send** and your large file will be uploaded to a folder in your **Sent** folder (in **Folders**) in Workshare. The recipient receives an email notifying them that file has been uploaded to Workshare online and providing a link to the file.

Chapter 4:   Working Online

This chapter describes the file share & sync element of your installation which brings the online secure file sharing, collaboration and storage features of Workshare to your desktop. It includes the following sections:

- **Overview**, page 72, introduces the online functionality available with Workshare.

- **Syncing local files**, page 72, describes how to use the Workshare desktop app to sync content between your desktop and Workshare online.

- **Getting content online**, page 78, describes how to share files to Workshare groups from open Office documents and using right-click options

Overview

With file share & sync included in your installation, you can add your files to the secure Workshare online platform. Once there, you can access your files from anywhere and share them securely with people inside or outside your organization.

Workshare integrates with File Explorer so you can save and organize your files in local folders that function seamlessly on your hard drive, but automatically synchronize with Workshare online. Workshare also integrates with Office so you can share for review, for example, from right inside Word.

Workshare is available online through a browser at my.workshare.com. Content is divided into different areas to suit your needs:

Folders   Use Folders to publish files and make them available to others. Within Folders, use My Files to store your own private files that you don't want to share with anyone but you want easy access to from anywhere.

Groups   Use groups as workspaces where you can collaborate on files with people inside and outside your company.

Workshare integrates its save and share functionality into your familiar working environment:

- Using the Workshare sync folder on your desktop, you can save and share any files to all areas of Workshare online

- From open Office documents, you can save files to My Files in Workshare and share files into Workshare groups

- From your desktop, you can right click any file and share it to a group in Workshare

In order to access and use Workshare online, you must have a Workshare account.

Syncing Local Files

The Workshare sync folder is your local access point to the online services of Workshare. Both the Workshare sync folder and the synchronization functionality are provided by the Workshare desktop app.
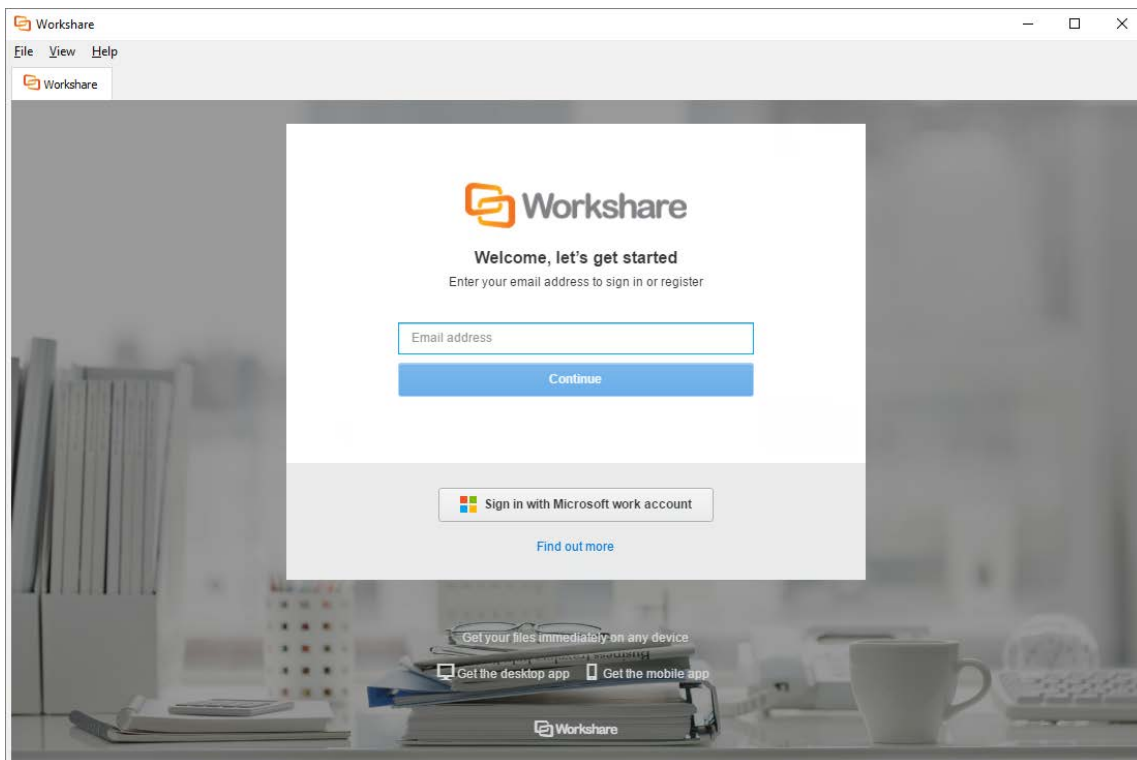
What is the desktop app?

With file share & sync included in your installation, the Workshare desktop application (the desktop app) is installed. This is an application that syncs content between Workshare online and your PC so you can access your files and continue collaborating from your desktop while offline. The key features of the desktop app are as follows:

- Synchronization - Synchronizes groups, folders and files between Workshare and your desktop. You can be selective about what is synchronized to reduce the storage footprint on your local machine. If you can't work online, as soon as you're back online, the new versions are uploaded right away.

- Integration - Integrates Windows with Workshare online linking Workshare directly to everyday applications – users can save files directly into the Workshare sync folder from where they are copied into Workshare online.

Launching the desktop app for the first time

The desktop app is launched once the Protect installation is complete.

The installation of the desktop app places an icon in your Windows taskbar for basic management and it puts a folder in your Favorites/Quick access section in File Explorer, so you can quickly access and save your Workshare content. In order to access and use the desktop app, you must log in to it. You only need to perform this login once; afterwards the desktop app will launch automatically when Windows starts. You use your Workshare login credentials to log in to the desktop app.

To log in to the desktop app for the first time:

- When the desktop app launches after installation, enter the email address and password you used to sign up for Workshare and click **Sign In**.

*Note: You can also display the login page by clicking the Workshare icon on your desktop or selecting **Workshare Desktop** from the Start menu.*

The Workshare desktop app looks very similar to Workshare online accessed from a browser.

In fact, from the desktop app, you can do all the things you can do when logging into Workshare online through a browser.

Once you have logged in:

- Your files and folders from your online Workshare account start to synchronize to your local Workshare sync folder
- The desktop app icon appears in your system tray

Workshare sync folder

The Workshare sync folder is your local access point to your online Workshare content. You can always find the latest copy of your Workshare files and you can add files to Workshare via the sync folder. It appears in your Favorites/Quick access section and its default location is C:\Users\[user name]\Workshare. You can change the location of the Workshare sync folder in Preferences > Sync Settings, described in *Configuring the Workshare Desktop App*.

You can also click **Open Workshare Folder** from the desktop app main window.

In your Workshare sync folder, you will see all your *synchronized* Workshare files and folders, grouped as follows:

- **Folders**: Shows all your Workshare files and folders, including files you have uploaded, as well as files others have shared with you. There are also three default folders:
  - **My Files**: Includes personal files that you don't want to share.
  - **Received**: Includes all the files sent to you by secure file transfer from Outlook.
  - **Sent Files**: Includes all the files you sent out to others by secure file transfer from Outlook.
- **Group Files**: Includes all your Workshare groups which are flexible workspaces ideal for projects that require dynamic conversations.

If you add, update or delete a file in your Workshare sync folder, it will be added, updated or deleted in Workshare online too. Similarly, if you add, update or delete a file in a synced folder in Workshare online through the web app on a browser, the changes will be seen in the Workshare sync folder.

The icon to the left of a file/folder indicates its sync status:

Waiting to be synchronized or synchronization is in progress

Synchronized

In this two-way file synchronization, updated files are copied in both directions, usually with the purpose of keeping the two locations identical to each other. You can control what is synced from your desktop just by adding or replacing files in your Workshare sync folder. Careful though, because anything you remove from your Workshare sync folder will also be removed from your Workshare online content.

Default sync

By default, the following files are synchronized:

- Files you add to My Files
- Files you add to a shared folder or a group that you own
- Files others add to a shared folder or a group that you own

You can select which folders to sync using the selective sync option. Refer to *Selective synchronization*.

System tray icon

The desktop app system tray icon shows the status of the desktop app as follows:

Icon	Status	Description
	Synced	The files in your local Workshare desktop folder are fully synced you're your online Workshare content.
	Sync in progress	The files in your local Workshare desktop folder are currently syncing with your online Workshare content.
	Pause	Synchronization between your local Workshare desktop folder and your online Workshare content is currently paused.
	Conflict	There is a conflict between files in your local Workshare desktop folder and files in your online Workshare content.
	Upgrade	An upgrade is available for the Workshare desktop app.
	Offline	The desktop app has been placed offline so no synchronization can occur.

Clicking the icon displays the following options:

Option	Description
Open Workshare App	Opens the Workshare desktop app window.
Open Workshare folder	Opens the Workshare sync folder.
Files up to date/conflicts	Indicates that all files are synchronized successfully or if there are sync conflicts between the desktop app and Workshare.
Pause	Pauses the current synchronization. The option becomes **Resume Syncing** when synchronization is paused.
Refresh	Refreshes the display and synchronizes with Workshare online.
Recycle Bin	Displays the Workshare recycle bin which includes all the Workshare files, folders and groups that have been deleted.
Selective Sync	Enables you to select which folders are synchronized between your desktop and Workshare online.
Preferences	Enables you to change application settings for the desktop app, such as the location of the sync folder or general account settings.
Help and support	Provides access to the Workshare knowledge base.
Quit Workshare	Stops the synchronization between your desktop and Workshare online.

Adding files to Workshare via the sync folder

You can add most file types to your local Workshare sync folder which will then be synchronized with your Workshare online account. You can add files to existing groups or folders or create new folders. You cannot create new groups from within the sync folder.

Note: Groups are created in Workshare from the web app or the desktop app.

You can simply copy/paste or save files into your local Workshare sync folder and they will be synchronized to Workshare online by default. However, if you have selected that specific folders do not synchronize then files added to those folders will not be synchronized. Refer to *Selective synchronization*.

To copy/paste to your local Workshare sync folder:

Drag the files or folders you want to add into your local Workshare sync folder.
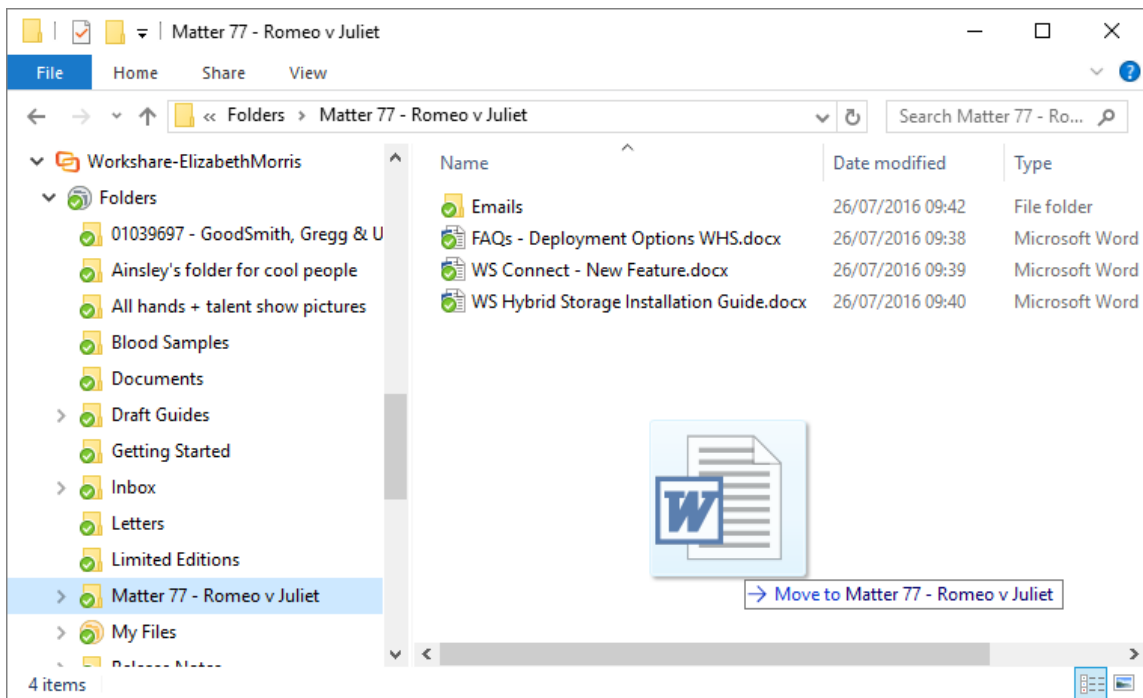
To save files to the Workshare sync folder:

1. Open a file – this can be any file, for example, a Word file, a PowerPoint presentation or an image file.

2. Click **Save As**.

3. Browse to your **Workshare** sync folder in Favorites/Quick access. By default this folder is located at Users\[user name]\Workshare.

4. Browse to a location in any of the three areas in Workshare and select an existing folder or create a new folder.

5. Click **Save**. Your file is now saved in your local Workshare sync folder and it is immediately synchronized to Workshare online (unless the selected folder is not set to synchronize).

Files won't sync from here…

- Files or folders added to the top level "Workshare" folder in your local sync folder will not be synchronized. Files and folders must be added into one of the two areas of Workshare – Folders or Group Files.

- New folders added to the Group Files area will not be synchronized – Groups can only be created via the web app.

In either of the above scenarios, the icon ![icon] next to the file and a popup message alert you that the file/folder cannot synchronize to Workshare.
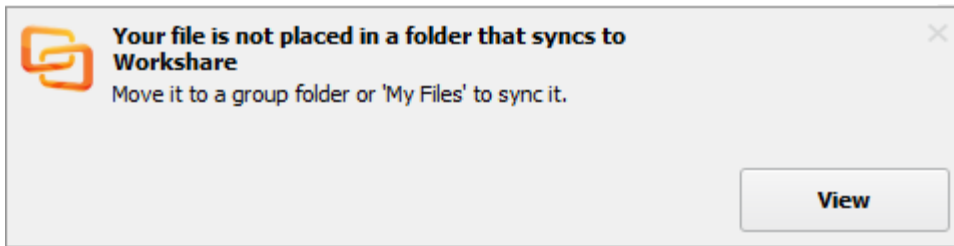
Clicking **View** opens the non-syncing folder locally so you address the problem.

Restoring deleted files

From the desktop app, you can access the Workshare online recycle bin where you can restore any of your accidentally deleted files, folders or groups. The recycle bin lists all your Workshare files and folders (those you own) that have been deleted – you may have deleted them using a web browser, from the desktop app or directly from the Workshare sync folder.

Note: When you have deleted files and folders from the desktop app or the Workshare sync folder, you will only see the deleted files and folders in the recycle bin after synchronization.

The desktop app provides a window into the Workshare online recycle bin so if you are offline, you will not be able to access the recycle bin.

To access the recycle bin:

Click **Recycle Bin** in the left panel.
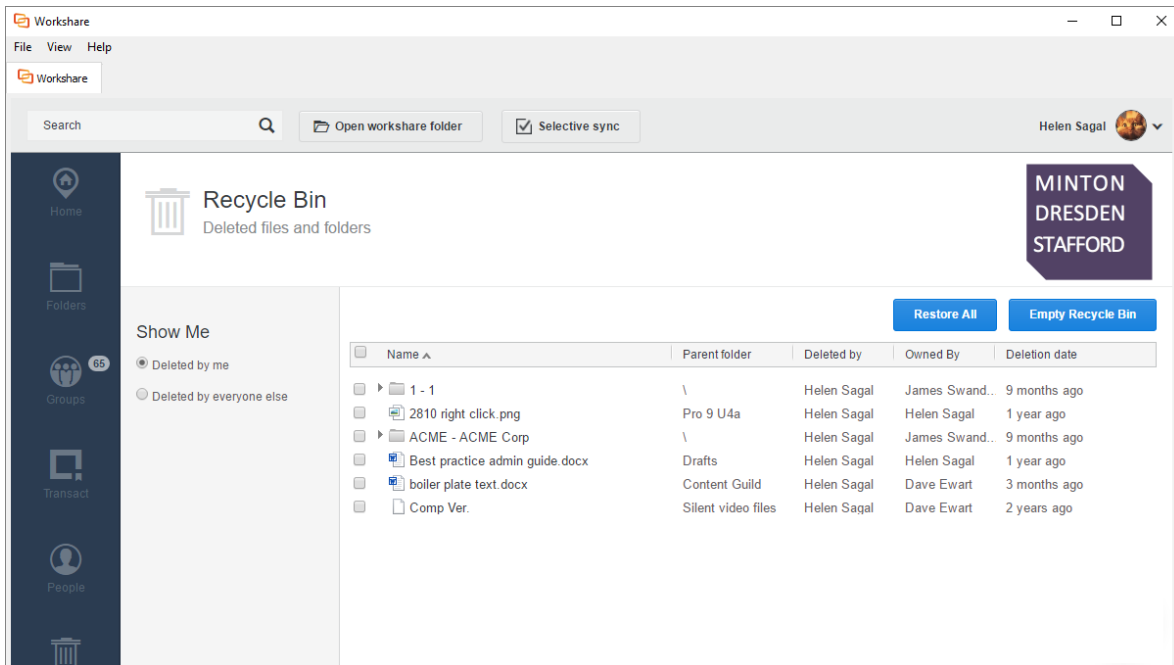
In the recycle bin you can see:

- Files, folders and groups owned by you that have been deleted by anyone; and
- Files, folders and groups owned by anyone that have been deleted by you.

You can filter the list to see what was deleted by you and what was deleted by others.

- Click **Restore All** to restore all files and folders in the recycle bin back to their original location.
- Click **Empty Recycle Bin** to permanently delete all files and folders in the recycle bin.

To restore selected files:

1. Click **Recycle Bin** in the left panel.

2. Select a file or a folder (or several files and folders). The buttons change to **Restore Selected** and **Empty Selected**.
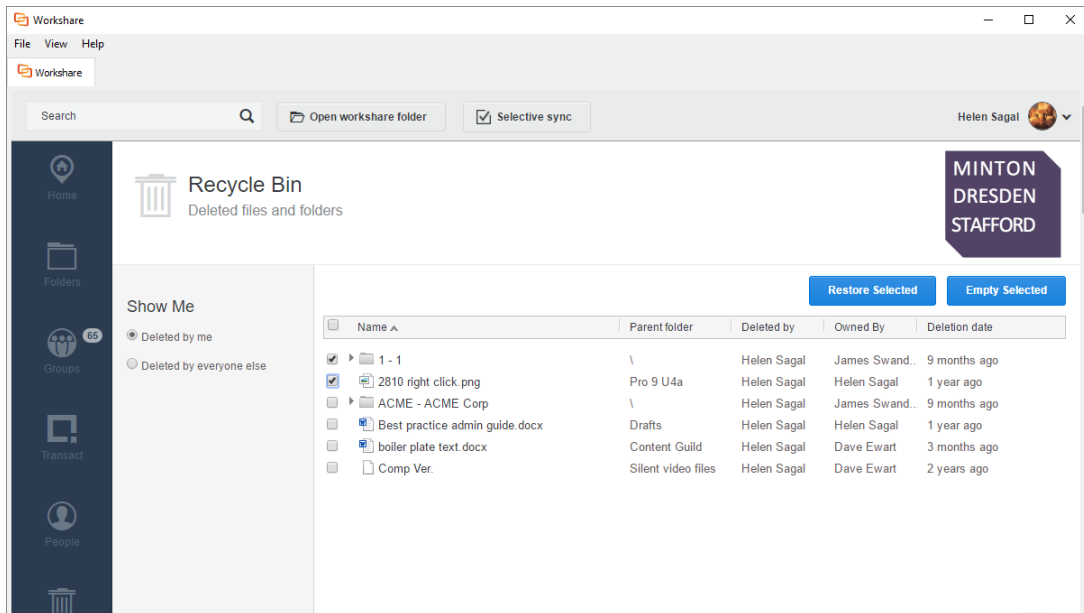
3. Click **Restore Selected** to restore the selected folders and files.

File synchronization

The desktop app synchronizes your online Workshare content to your local machine so you can access your files and continue collaborating when offline. By default, the following files are synchronized:

- Files you add to My Files

- Files you add to a shared folder or a group that you own

- Files others add to a shared folder or a group that you own

So if you add any of these files to Workshare via a web browser, they will be synced to your desktop and you will be able to access them from the Workshare desktop app (or sync folder). Synchronization works both ways so if you delete any of these files from the Workshare desktop app (or sync folder), they will be deleted from Workshare online and you will no longer be able to access them via a web browser.

Synchronization between Workshare online and your desktop occurs in the following situations:

- When logging into the desktop app

- When a new event occurs on Workshare online, such as a new file uploaded or a new version added

- When a new event occurs in the Workshare desktop app (or sync folder), such as a new folder created or a file added

- When the desktop app has been offline and then you go back online

- When clicking **Refresh** in the desktop app system tray menu

- When clicking **Update and Sync** in the Selective Sync page

You can pause synchronization at any time, for example, if you have a slow connection, and then restart it when convenient.

To pause synchronization:

Click the desktop app system tray icon and select **Pause**. Synchronization stops.

To restart synchronization, click the desktop app system tray icon and select **Resume**.

Selective synchronization

You can modify the default synchronization settings so that less files and folders are synchronized to your desktop in order to reduce the storage footprint on your local machine.

To select folders to synchronize:

1. Click **Selective Sync** in the desktop app main window (or from the desktop app system tray menu or the *File* menu). The selective sync page is displayed showing the root folders on Workshare – **Folders** and **Group Files**.

2. Click a folder to display its subfolders.

3. Select the folders that you want to synchronize between Workshare and your desktop by selecting the checkbox to the left of the folder/subfolder name. Selecting or deselecting a folder will automatically select/deselect the subfolders belonging to the folder. However, you can select a folder but then manually deselect some of its subfolders. Use the **Select All** checkbox to quickly select/deselect all folders.

   *Note: By default when a folder or group is shared with you it is not selected for synchronization. To change this, select the **Automatically sync new folders shared with me** checkbox.*

4. Click **Update and Sync**. All folders with a selected checkbox will be synchronized. The progress of the synchronization is shown in the sync progress page.
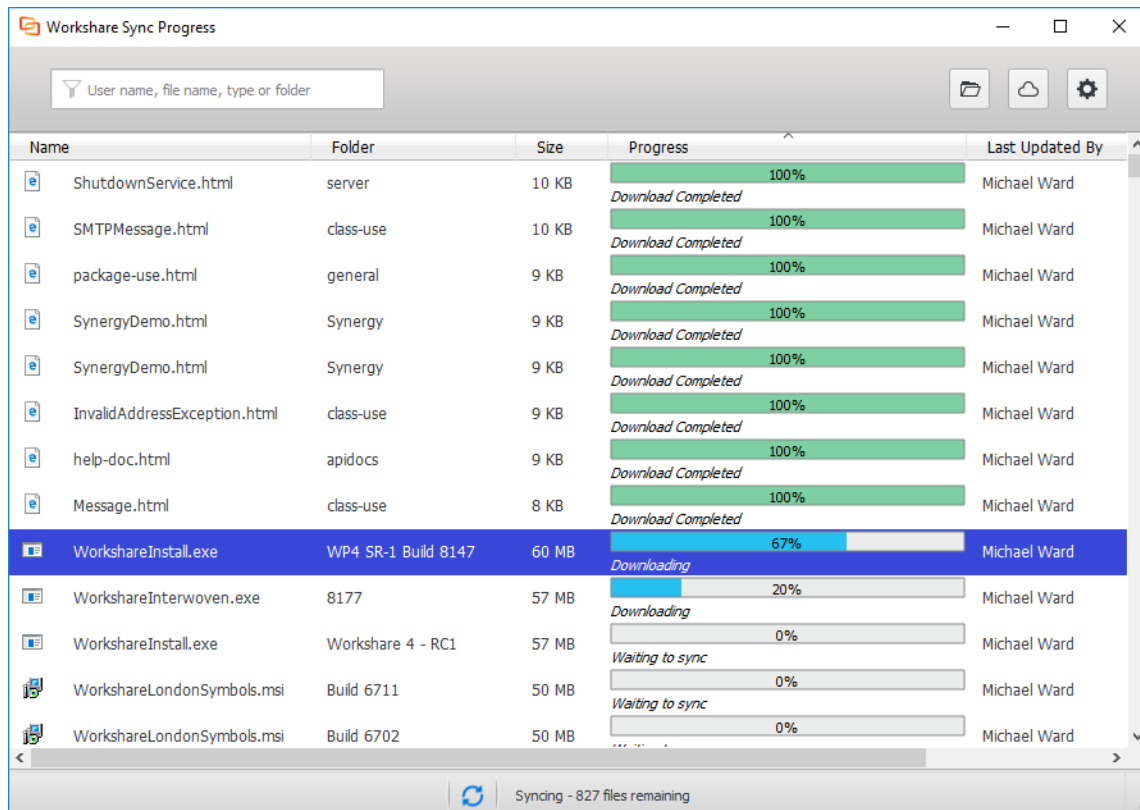
Folders that are not synchronized will not appear in your local Workshare sync folder.

Sync progress

The sync progress page shows the folders and files currently being synchronized.

To display the sync progress page:

When synchronization is in progress, select **Sync Progress** from the View menu.

The status bar provides a summary of the sync situation and the sync progress report provides a detailed view.

The files being synchronized are shown in a queue format. If you want to move a file in the queue, for example, you want to upload a small Word document and it is being held up by a large PowerPoint presentation, right-click the file you want to delay and select **Lower the sync priority**.

Synchronization conflict

The sync conflicts page provides a dedicated area where you can deal with file conflicts. Possible conflict scenarios include:

- You have opened a synced file locally and you are editing it. Meanwhile, in the web app, a new version is added to the file. When you save the open file, a conflict is shown.

- Two users are working offline and make changes to a file they share. User 1 goes back online and the revised file is synced to Workshare online as a new version. User 2 goes back online and a conflict is shown.

In your local Workshare sync folder, the file icon shows there is a conflict:
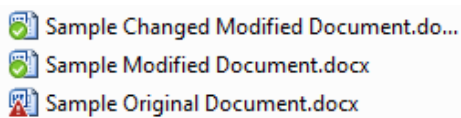
In addition, the desktop app system tray icon shows there is a conflict and the menu includes a **Conflicts** option:
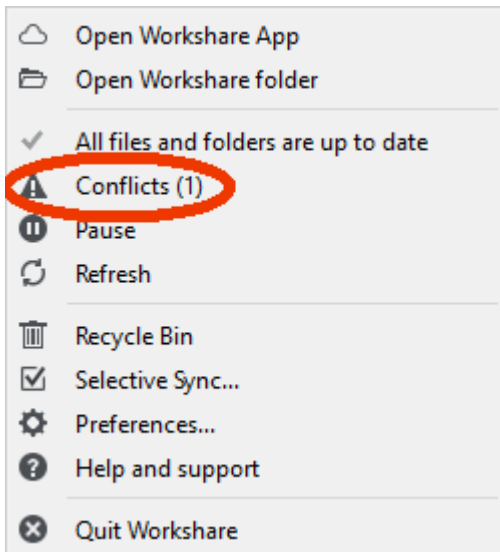
To resolve a conflict:

1. Click **Conflicts** in the desktop app main window (or from the desktop app system tray menu). The sync conflicts page is displayed listing the files with conflicts.

2. Expand a file in the sync conflicts page by clicking ⌄. The options for resolving the conflict are displayed. For example, you may want to add your file as the latest version or overwrite your version with the online version. You can always opt to keep both files involved in the conflict. Different options are displayed according to the particular conflict.
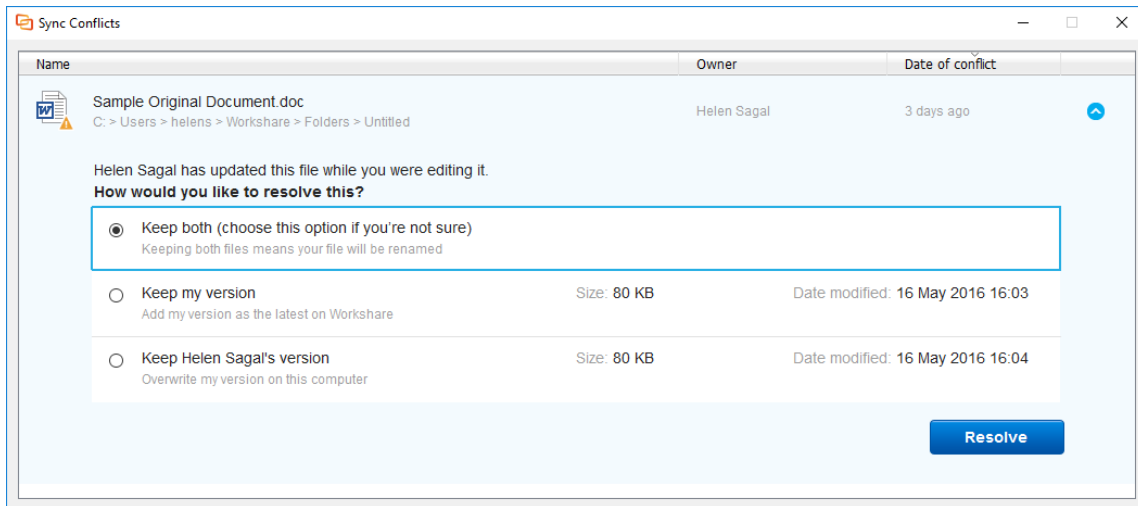
3. Select the option you want to apply and click **Resolve**.

Note: When there are no conflicts, the sync conflicts page is not available.

Collaborating in Workshare

Once you have shared folders with other users, those users will be able to access Workshare via the web app, view the files in the folder and add comments in real-time. If they have permission, they could also add new versions to a file. Any new versions will be synchronized to your desktop and you can also add versions to Workshare files from your desktop through your Workshare desktop app or your local Workshare sync folder. For example, simply open a file from your local Workshare sync folder, edit it and save it and it will be synced to Workshare online and appear as a new version.
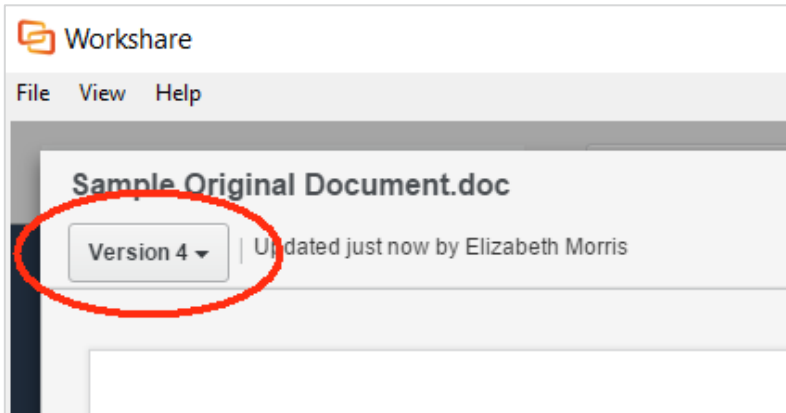
You can also open any file and save over a file in your local Workshare sync folder. It will be synced to Workshare online and appear as a new version.

Getting Content Online

As well as using your local Workshare sync folder to get your content online, you can use the right-click options and toolbar options added by the file share & sync element of your Protect installation.

Right-click sharing

The way to share files and folders from your desktop is to share them to a Workshare group.

Right-clicking any file on your desktop provides the option to share it to a group. The file or folder will be added to the group's files and all members of the group will be able to access it.
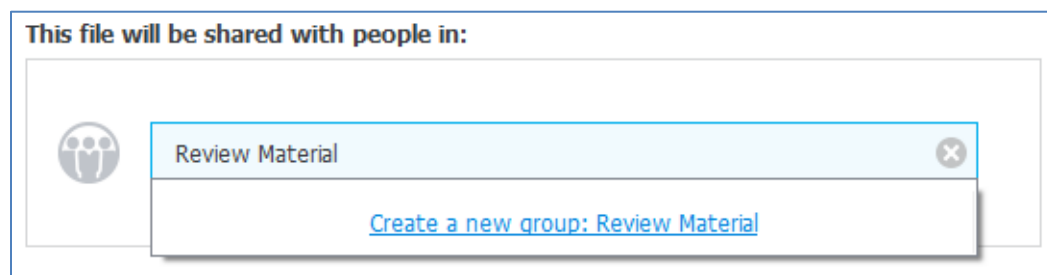
To share to a group:

1. In File Explorer, right-click any file or folder.
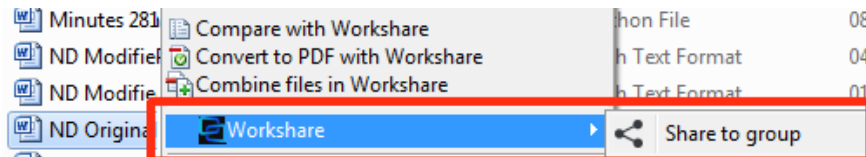
2. Select **Workshare**, then **Share to group**.
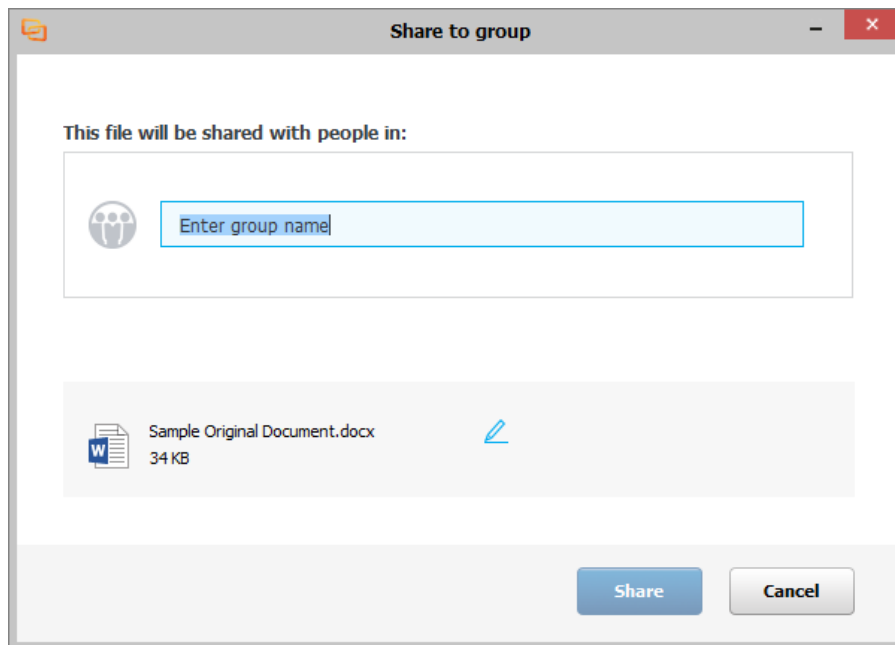
3. Enter the name of the group you want to share the file/folder with. When you click in the text box, a list of the most recent groups selected is displayed. As you start to enter a name, groups are suggested to you.

4. Select an existing group or enter a new group name and click **Create a new group**.

> **Note**: Click **Change Group** to remove the specified group so you can select another one.

5. If you want to change the name of the file/folder you are sharing, click and edit the name.

6. Click **Share**. The file/folder is uploaded to the specified group in Workshare online. If the group is synced, the added file or folder will also appear in the selected group in your local Workshare sync folder.

From open Office documents

Using Workshare toolbar options, you can save your Office files to Workshare online so they will be accessible to you online at all times. You can save them directly to a folder in My Files if they are private files that you don't want to share with anyone or you can save them directly to a group if you want to collaborate on them with people inside and outside your company.

You can save Word, Excel and PowerPoint files in their native format or convert them to PDF as you save.

Additionally, you can display the Workshare Connect panel inside Office which provides a window into the document you have shared to a Workshare group.

Saving to My Files

The My Files area of Workshare online is where you can securely store your own private files that you don't want to share with anyone but you want easy access to from anywhere.

To save documents to My Files:

1. Open a file in Microsoft Word, Excel or PowerPoint.

2. In the Workshare tab, click **Save to My Files**. The *Save to My Files* dialog is displayed.
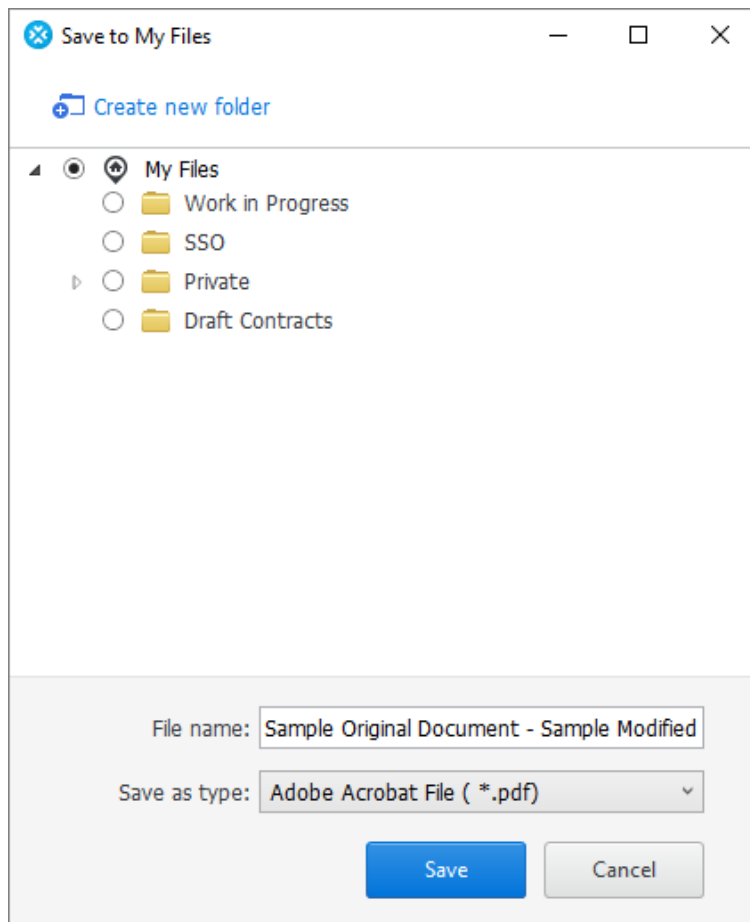
> ***Tip!*** *You can also display this dialog using Workshare options in the File menu.*

3. Browse through My Files and select the folder where you want to save the file.

> ***Note***: *To create a new folder, click **Create new folder**, enter a name for the folder and click **Create**.*

4. In the **File name** field, modify the name of the file as required.

5. From the **Save as type** dropdown list, select the format for the saved file from the following:
   - **Word Document/Excel Workbook/PowerPoint Presentation**: Saves the file in its native format
   - **PDF**: Saves the file as a PDF file
   - **PDF/A**: Saves the file as a PDF/A file

6. Click **Save**. The file is saved to the specified folder in Workshare My Files and you can log into Workshare and access the file from anywhere. The following notification pops up on your desktop:

You can click **View** to open the file in Workshare in your browser or click **Copy link** to copy the URL to the file to your clipboard. You can then paste this link to another location, for example, an email or an instant message.

If the Workshare My Files folder is synced, the added file or folder will also appear in your local Workshare sync folder

Once you have saved a file to My Files, you can continue working and making changes as required. Clicking **Save to My Files** again will save the file to Workshare with the same name and in the same location as a new version. If you want to save the file to My Files as a new file with a different name, click the arrow on the **Save to My Files** button and click **Save as**.

Sharing to a Workshare group

By sharing files to Workshare groups, you save your file to a group in Workshare and all members of that group can access your file and collaborate on it with you.

To share documents to a group:

1. Open a file in Microsoft Word, Excel or PowerPoint.

2. In the Workshare tab, click **Share**. The *Share* dialog is displayed.
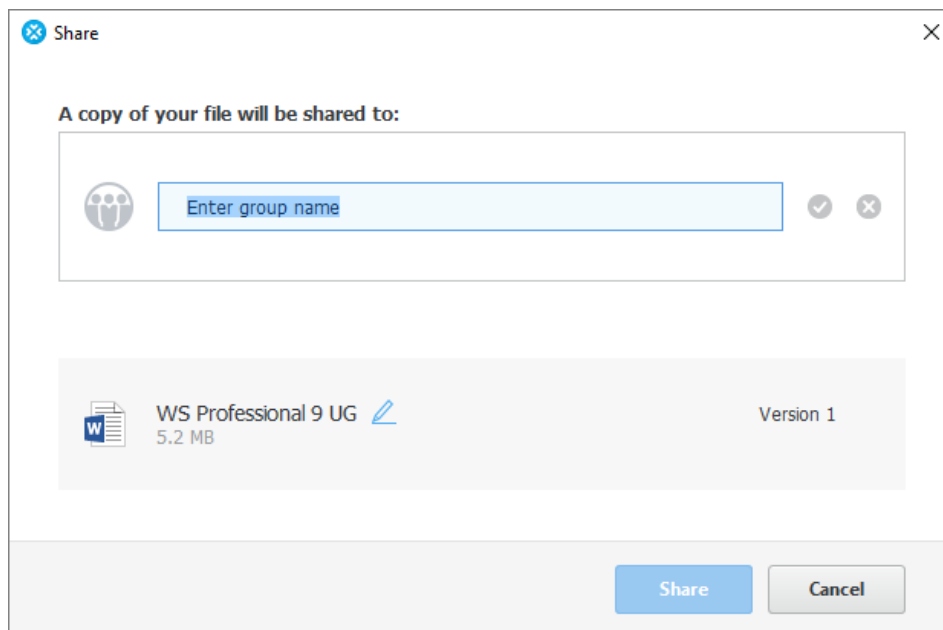
> *Tip!* *You can also display this dialog using Workshare options in the File menu.*

3. Enter the name of the group you want to share the file with. As you start to enter the name, groups are suggested to you.
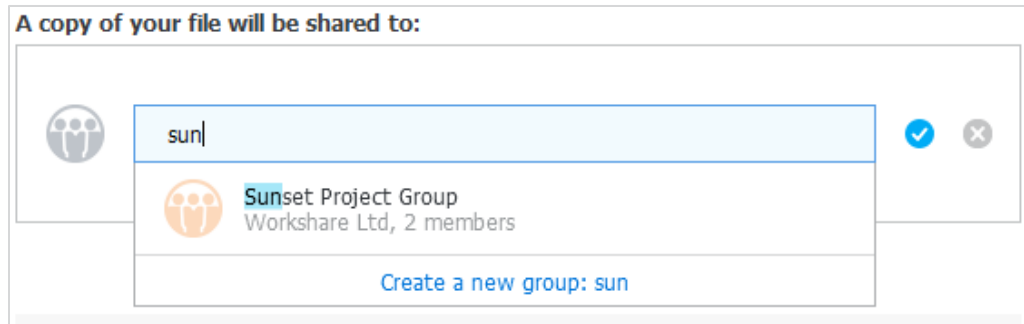
4. Select a group or enter a new group name and click **Create a new group**.

5. Edit the name of the document by clicking ✎ , modifying the name and then clicking ✅ .

6. Click **Share**. The document is saved to the group in Workshare and a confirmation dialog is displayed.
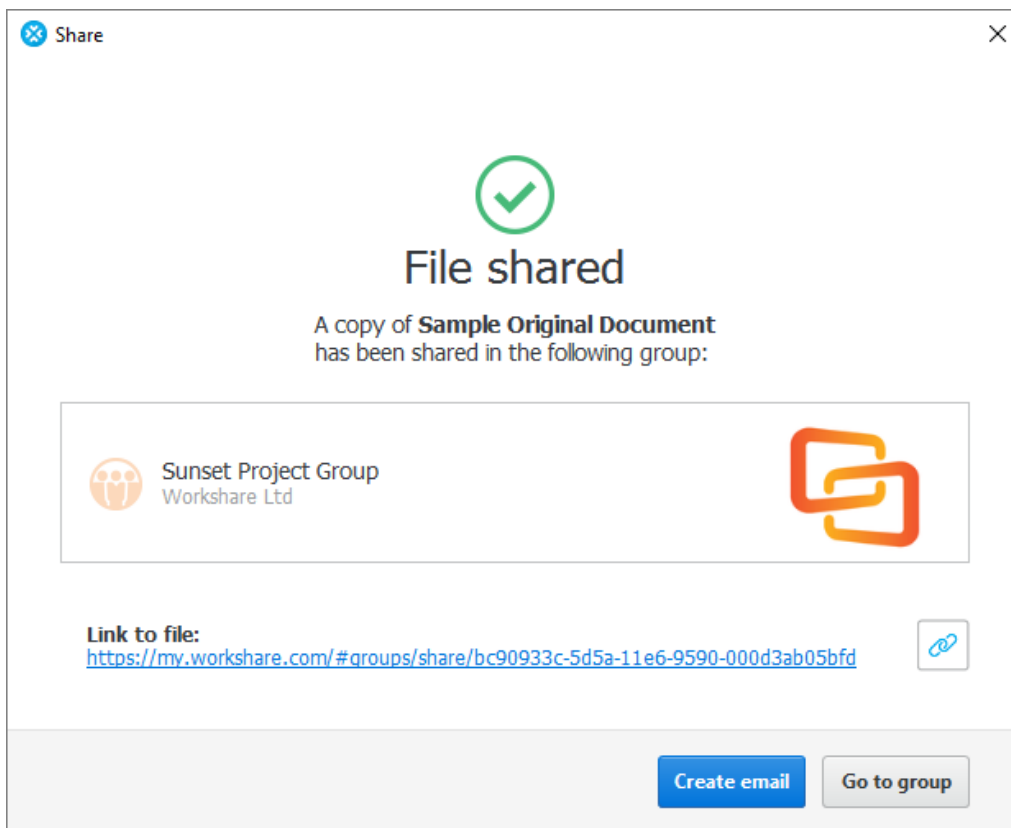
If the Workshare group is synced, the added file or folder will also appear in your local Workshare sync folder

7. Continue in one of the following ways:

   ▫ Click **Create email** to open a new email in Outlook that includes a link to the document in Workshare. You can invite people to the group by sending the email to them.

   ▫ Click **Go to group** to open the group in Workshare in your browser where you can see the document, set group permissions and select members.

Note: Click *to copy the link to the document to your clipboard. You can then paste this link to another location, for example, an email or an instant message.*

Monitoring shared files

The Workshare Connect panel inside Office provides a window into the files you have shared to Workshare groups.

When you have shared a document into a group in Workshare and you open the document locally, the Workshare Connect panel provides a view of what is happening with your collaboration. You can see the other reviewers (the members of the group) and whether they are online at the moment. You can also see how many comments have been made on the document and whether any new versions have been added to it. With a single click you can open the document in Workshare online via a browser and join in the collaboration by viewing comments and making your own comments.

If you open a shared document in Office and the Workshare Connect panel is not displayed, click **Toggle Panel** in the Workshare tab to display it. When the document is not shared to a Workshare group, the panel will look something like this:
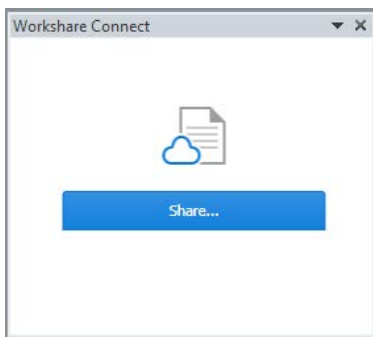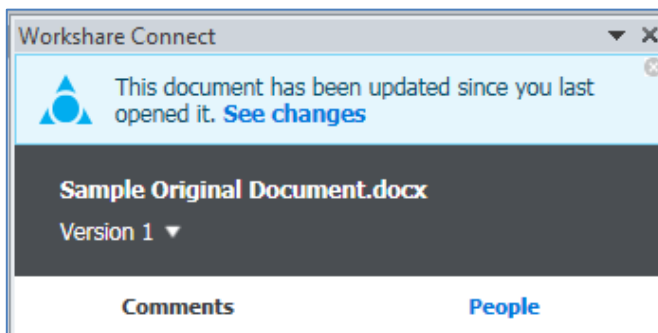
Once your document is shared, the Workshare Connect panel will provide real-time information about the collaboration, like new comments and versions.

Click the version dropdown to see other versions of the document. Click a version to display it in the Workshare web app.

A new version has been uploaded. Click here to download it.

The **People** tab shows the members of this group and who is reviewing and editing the document.

The **Comments** tab shows the number of comments made on the displayed version as well as the total number on all versions.

When there are comments you have not yet read, click this alert to display the document in the Workshare web app so you can review the comments.

Click here to display the document in the Workshare web app.

Workshare Connect

A new version of this document is available. **Download**

Sample Modified Document..docx
Version 1 ▼

Comments   People

Unread comments   >

4

Comments on this version

Total of 6 on this document

View online

New versions

When another group member adds a new version of the document, you are notified in the Workshare Connect panel. Click **Download** and the new version is downloaded and opened. Now the Workshare Connect panel will ask if you'd like to see what's different between this new version and the previous version. With a single click, both versions are compared in Workshare Compare.

Workshare Connect

This document has been updated since you last opened it. **See changes**

Sample Original Document.docx
Version 1 ▼

Comments   People

Comments added

In the **Comments** tab, you can see the number of comments made on the version of the file you are looking at (in orange) as well as the total number of comments on all versions of the file. If you want to see the actual comment, click **View online** and open the file in Workshare via a browser so you can view comments and update versions and add comments if you want. When comments are made that you have not yet seen, click the **Unread comments** alert and the file is opened in Workshare via a browser.

Group members

In the People tab, you can see all members of the group that have access to your document. A green light indicates the member is currently viewing the file. The following three lists are available:

- **Everyone**: All members who have access to the file
- **Reviewers**: Any member who has looked at the file
- **Editor**: A member who has looked at the file in Word (and had Protect installed and the Connect panel turned on)

Chapter 5:   Advanced PDF Functionality

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

- **PDF Combine**, page 95, 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.

Protect supports the combination of the following file types into a single PDF file: DOC, DOCX, PPT, PPTX, XLS, XLSX, PDF, RTF, TXT, HTML, MSG.
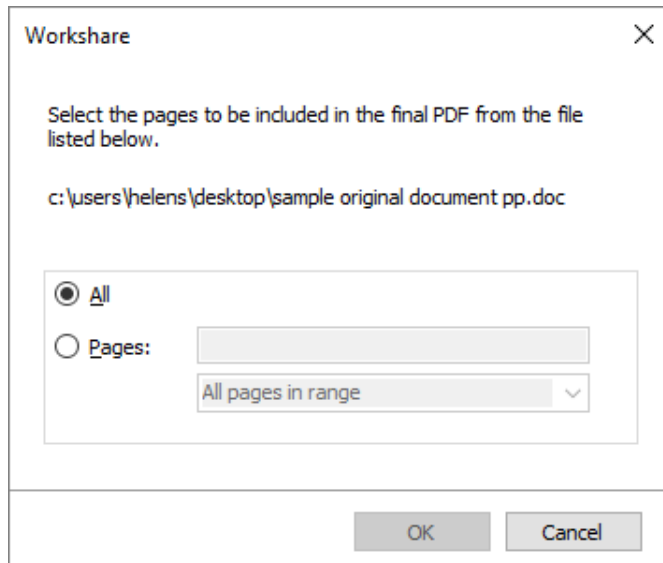
To combine multiple documents into a single PDF:

1. In an open Office document, click **Combine PDF** (**Protect** group) in the Workshare 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.
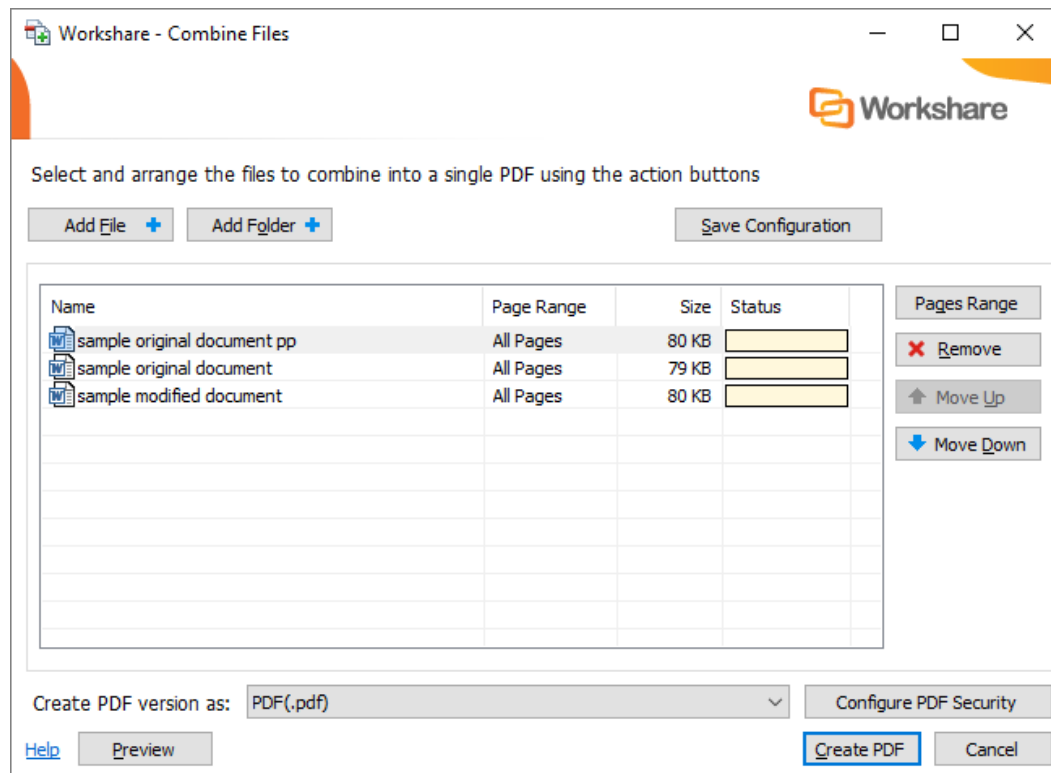
2. Add the additional files you want to include in the single PDF using the buttons at the top or by dragging and dropping. Click **Add Files** to select and add a single file and click **Add Folder** to add multiple files from a selected folder.

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:

All pages in range ⌄

OK   Cancel

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**.

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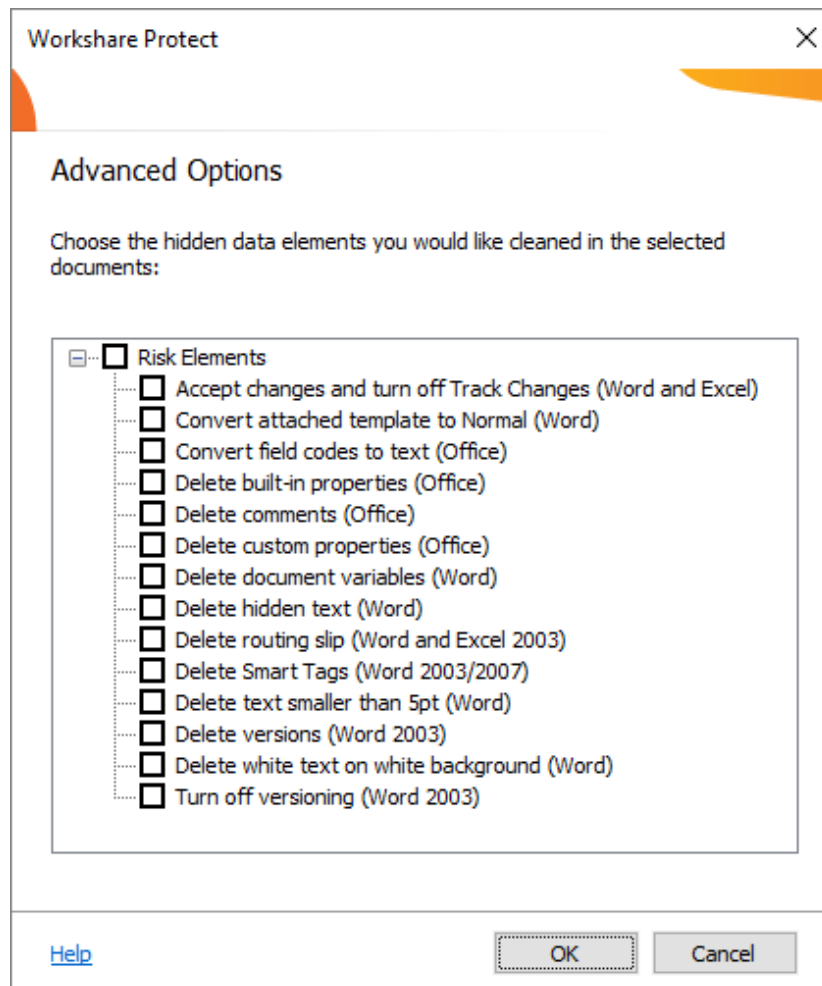
11. Select hidden data elements as required. For a full description of all the hidden data elements, refer to *Cleaning Hidden Data* for further information.

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.

Note: If you work with Workshare online, you can also use Save As and save the combined PDF to your Workshare sync folder and it will be synchronized to Workshare. Refer to Adding files to Workshare via the sync folder..

Chapter 6: Configuring Workshare

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

- **Introducing the Workshare Configuration Manager**, page 101, introduces the Workshare configuration utility.

- **Accessing the Workshare Configuration Manager**, page 101, describes how to access the Workshare Configuration Manager.

- **Setting Parameters**, page 103, 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 *Workshare* tab or from the Start menu, select **Workshare Configuration (User Mode)**. The Workshare Configuration Manager opens in User Mode.
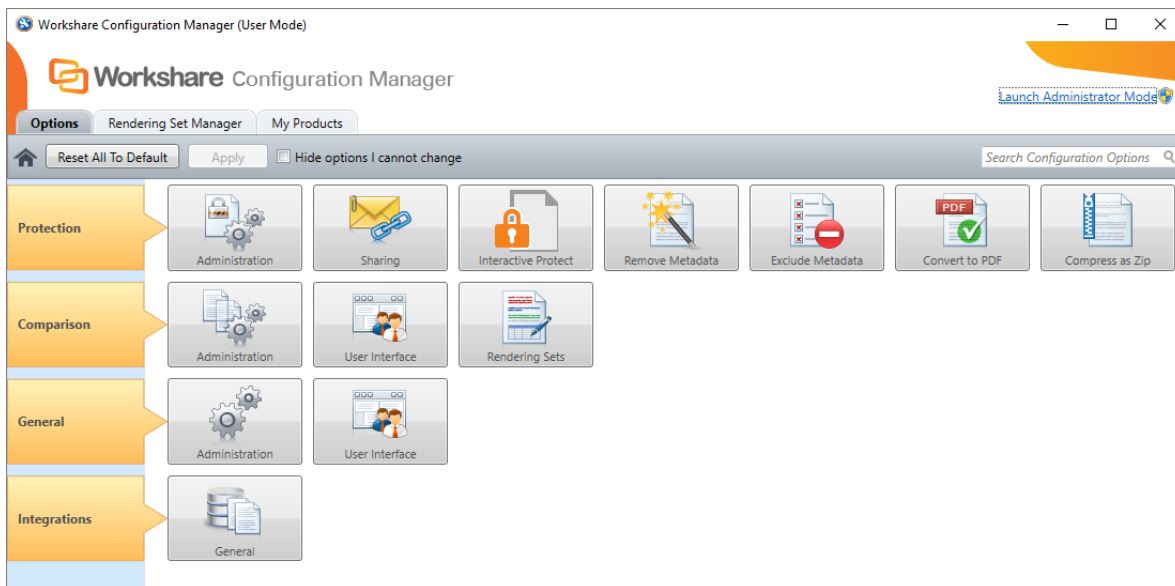
> **Note**: *In User Mode, the state of the options reflects the settings in HKEY_CURRENT_USER in the Registry.*

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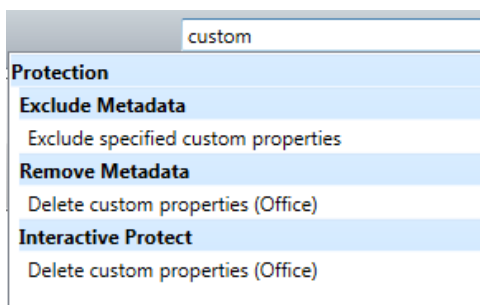
Click the parameter in the results list and the relevant category and sub-category is displayed in the Workshare Configuration Manager.

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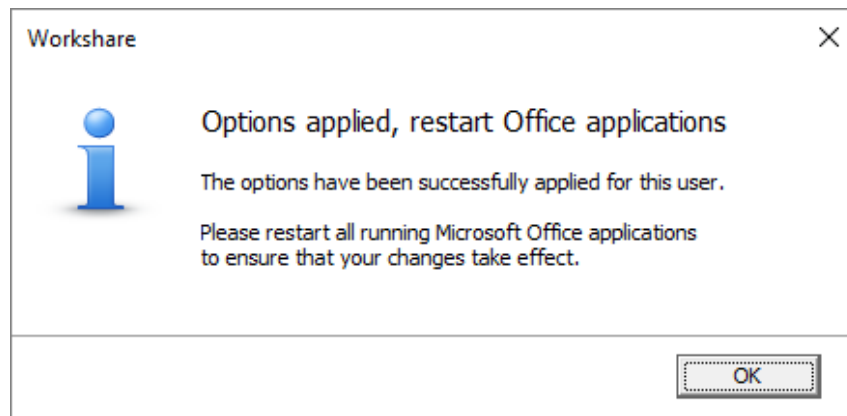
5. Click **OK** and restart all Microsoft Office applications.

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

# Appendix A. Configuring Workshare Desktop App

This appendix describes how to configure the Workshare desktop application (the desktop app). This is an application that syncs content between Workshare and your PC so you can access your files and continue collaborating from your desktop while offline.

Configuring the Workshare Desktop App

You can configure application settings for the Workshare desktop app, such as the location of the sync folder or general account settings.

To configure the Workshare desktop app:

1. Click the desktop app system tray icon and select **Preferences** or from the *File* menu in the desktop app main window, select **Preferences**. The following dialog is displayed.
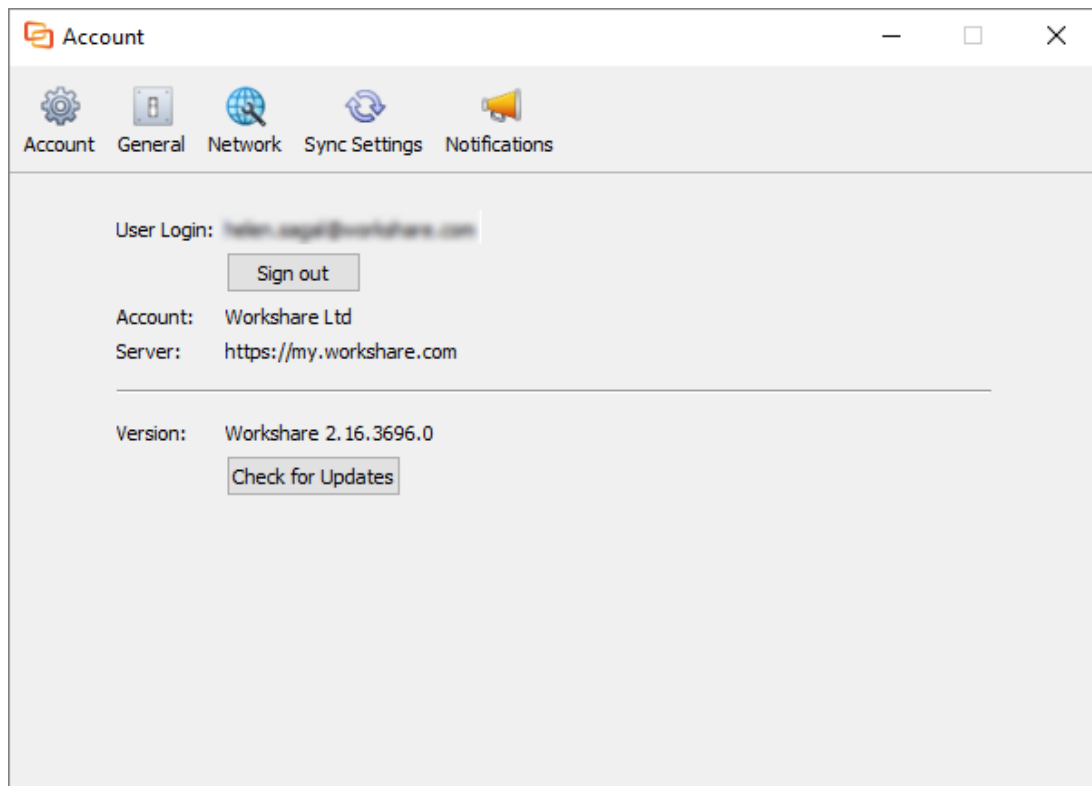
The **Account** page provides information about your account. You can see your registered Workshare email address that you use to log in to Workshare as well as the address to the Workshare server. Additionally, you have version information about the desktop app.

2. Select **General**.
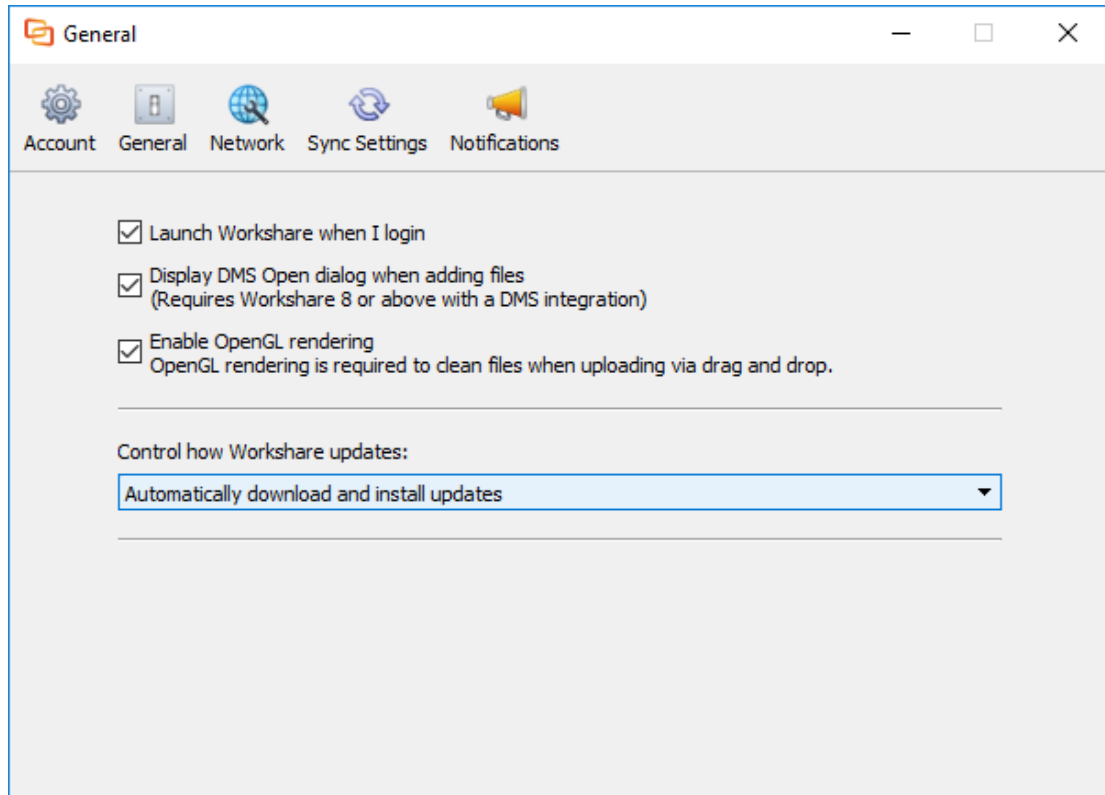
3. Select the **Launch Workshare when I login** checkbox and the desktop app will start when your computer is started.

4. When you have Workshare 9 (or above) with a DMS integration, select the **Display DMS Open dialog…** checkbox and you can select files from your DMS when uploading files to Workshare from the desktop app.

5. By default, the desktop app uses off-screen rendering (OpenGL rendering). In cases where off-screen rendering is not supported (for example, GPUs with older graphics drivers), the desktop app will automatically switch to on-screen rendering. If the desktop app cannot recognize that there is a problem with off-screen rendering, you can manually switch to on-screen rendering by deselecting the **Enable OpenGL rendering** checkbox.

> *Note: When using on-screen rendering, the clean/convert options will not be available when using drag and drop to add files. For more information about OpenGL rendering, refer to this article in the Workshare knowledge base.*

6. To control how Workshare updates, select from the dropdown:
    □   **Automatically download and install updates**: Updates to the desktop app will be downloaded and installed automatically as they become available.
    □   **Notify me when updates are ready to install**: You will be notified when updates to the desktop app are available.

7. Select **Network**.
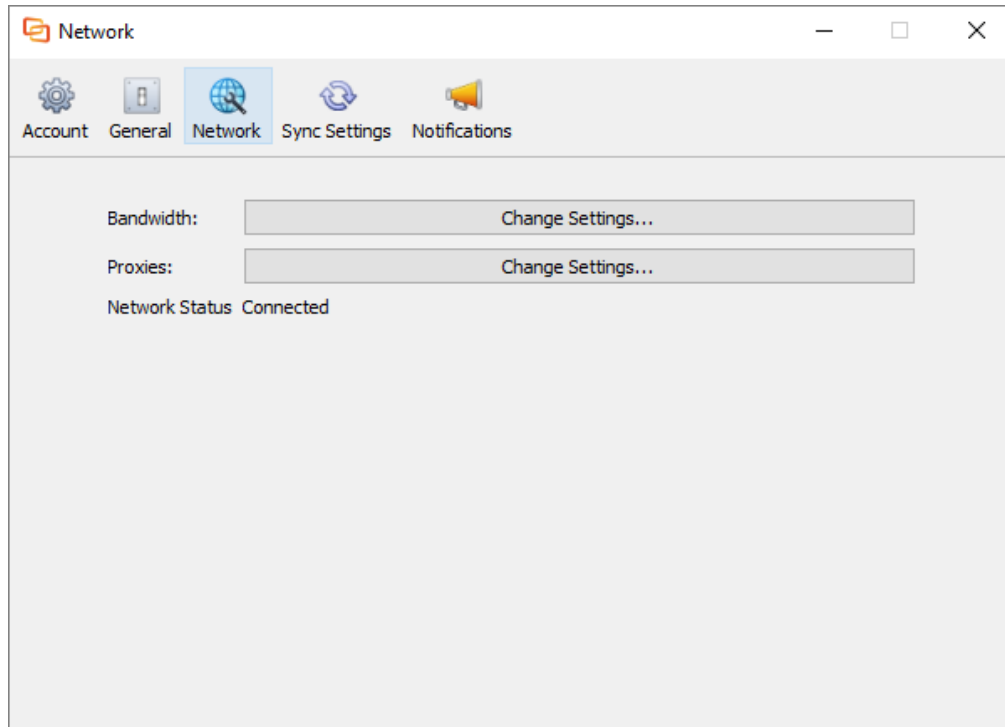
The Network page enables you to limit bandwidth settings and change the settings of your proxy server.

8. In the **Bandwidth** field, click **Change Settings**.
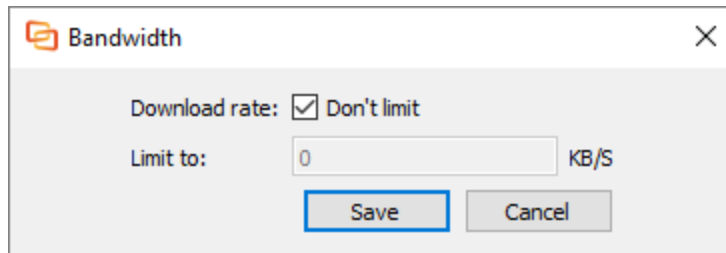
9. If you want to limit the bandwidth available to data downloaded to the desktop app, deselect the **Don't limit** checkbox and specify the limit in the **Limit to** field.

10. Click **Save**.

11. In the **Proxies** field, click **Change Settings**.
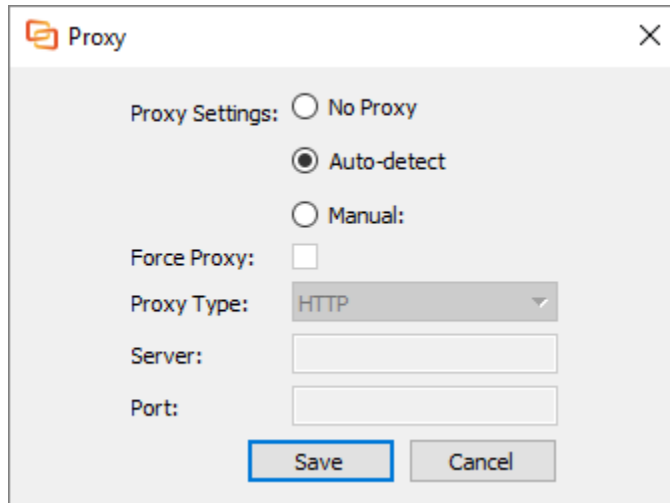
12. When working with a proxy server, select **Auto-detect** and Workshare will use your computer's system settings to connect to the network, or select **Manual** and enter your proxy server details manually.

> *Note: There is no **Auto-detect** option available when working on a Mac.*

13. When manually specifying proxy server settings, you can select **Force Proxy** so that the desktop app traffic MUST go via your proxy server and if the proxy server is not available then the desktop app will be offline.

14. Select the type of your proxy server (**HTTP**, **HTTP Caching** or **Socks5**) and enter the server address and port number.

15. Click **Save**.

16. Select **Sync Settings**.
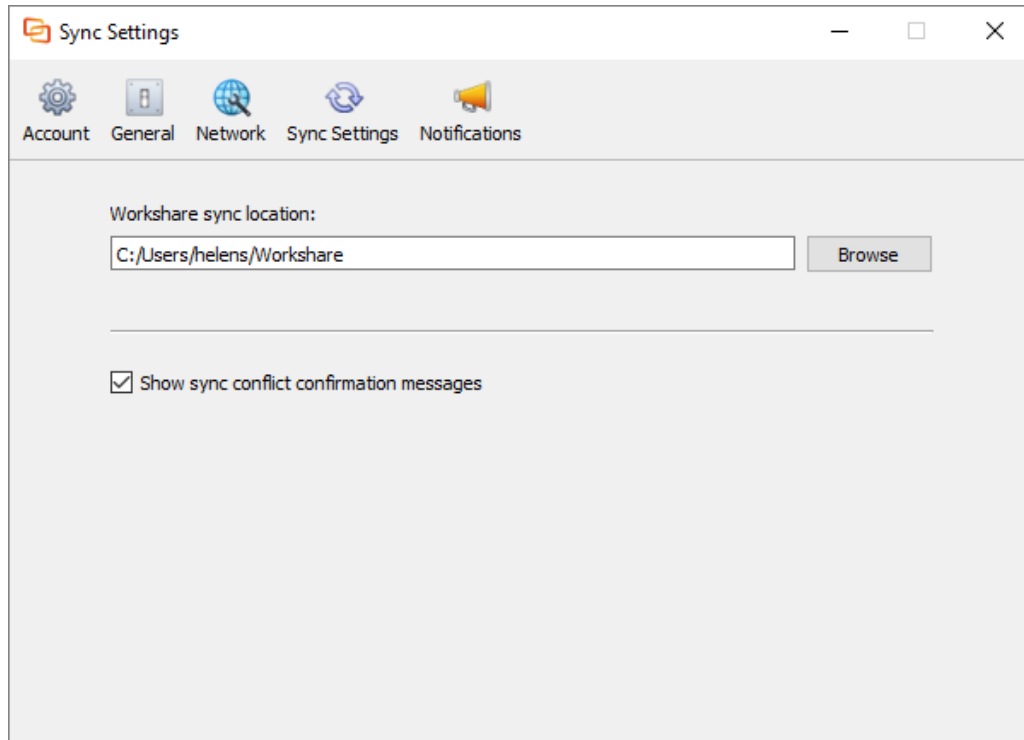
17. If required, change the location of the Workshare sync folder by clicking the browse button and selecting a different location. By default, this folder is named and located as follows:
    ▫ Windows: C:\Users\[user name]\Workshare
    ▫ Mac: /Users/[user name]/Workshare

    Any files or folders put in this folder will be synced to Workshare online and will appear in the desktop app.

18. Select **Notifications**.
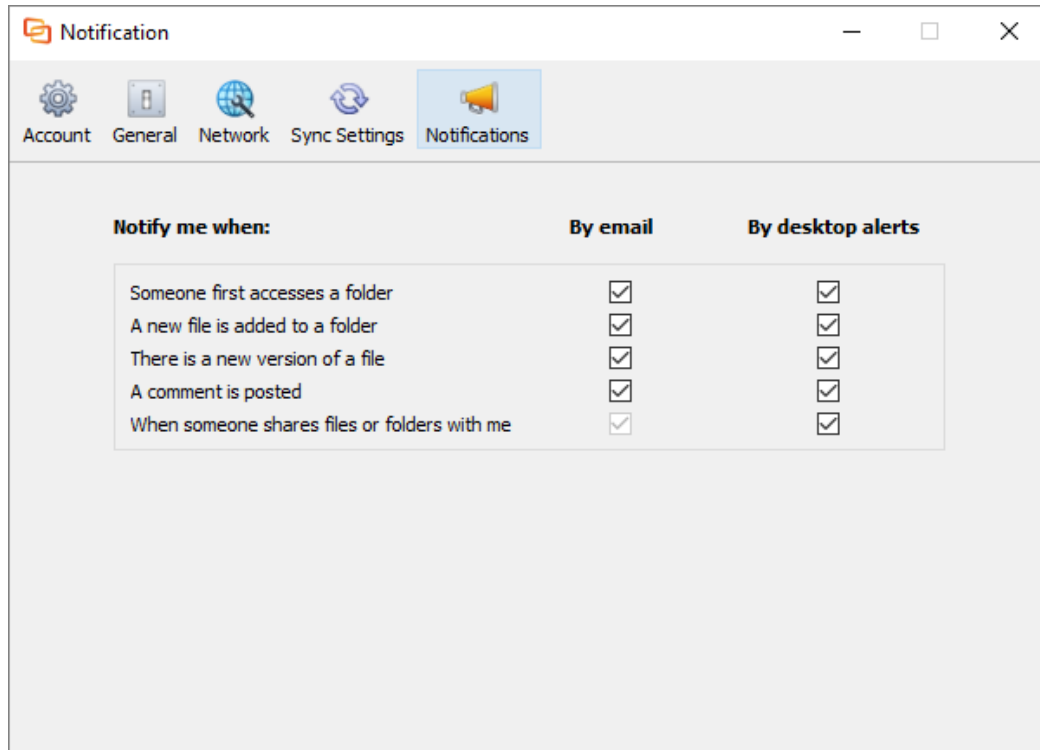
19. If required, change the notification settings. By default, users receive notifications by email and via desktop popup alerts in the following circumstances:
    ▫ When a user first accesses a folder you have shared with them
    ▫ When a new file is added to a shared folder
    ▫ When there is a new version of a file
    ▫ When a comment is posted
    ▫ When someone shares a file or folder with you