GUIDE

Workshare Protect

Getting Started Guide

Workshare

Introducing Workshare Protect

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

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

Note: *This guide is designed to quickly get Microsoft Office users started with Workshare Protect. This guide introduces the main functionality of Workshare Protect but for a more detailed description of its functionality and capabilities, please read the Workshare Protect User Guide. This Guide and further information is available on the Workshare website. To contact Workshare Technical Support, please log a case via the web at http://www.workshare.com/support/.*

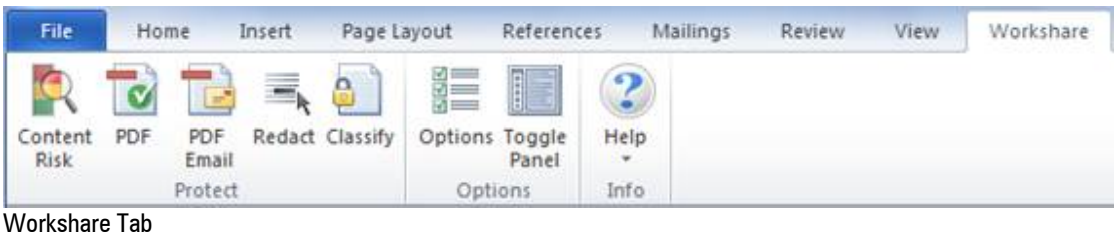
Workshare Environment

Workshare Panel

Workshare Protect integrates into your existing Microsoft Office environment. A panel appears on the left of the active document and a *Workshare* tab appears in the Ribbon (MS Office 2007) or a *Workshare* menu appears in the menu bar (MS Office 2003). You can show/hide the Workshare Panel by clicking **Toggle Panel** in the *Workshare* tab (MS Office 2007) or by selecting **Show Workshare Panel** from the *Workshare* menu (MS Office 2003).

***Note**: In MS Office 2003, Workshare Protect can also be configured so the Workshare menu is replaced with the Workshare toolbar.*

Workshare Menu



Workshare Tab

Check and Alert to Content Risk

Workshare Protect alerts you to content risk (content that violates company security policies) in your documents. Workshare Protect enables the discovery of content risk in the following ways:

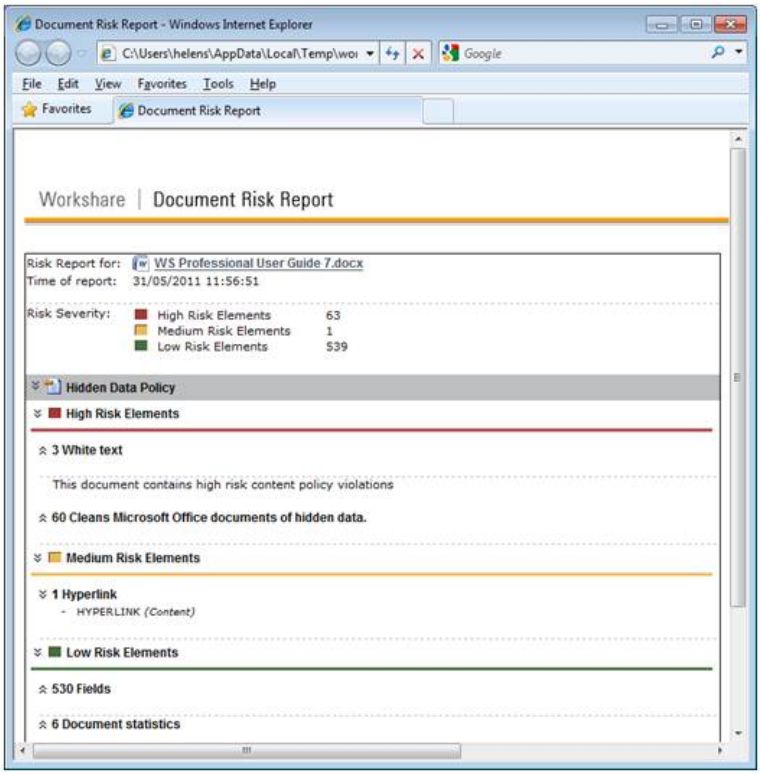
- **Content Risk Reports**: Workshare Protect integrates with Microsoft Office providing an option to display a comprehensive report of all the content risk in a document while it is open in Microsoft Office.
- **Email Protection**: Workshare Protect prevents users from accidentally emailing confidential information by alerting users before the email is sent when an email or its attachment breaches security policies. Depending on the actions defined for policy breaches, emails may be blocked or sensitive data removed.

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

How to:

Generate a report on content risk:

1. Open your document and click **Content Risk** in the Workshare Panel. Workshare Protect displays a summary of the content risk contained in the document.
2. Click **Report**. The Report Wizard is displayed.
3. Click **Next**, select the report format (XML or HTML) and click **Next**.
4. Click **Finish**. The Risk Report is displayed showing all instances of hidden data.



Sending Secure Emails

Workshare Protect is able to process the emails you send and remove metadata from attachments or convert attachments to PDF. Whether Workshare Protect processes your emails is determined by the configuration settings. 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 sending emails you may see the Protect Profile dialog or the Email Security dialog.

How to:

Send secure emails using the Protect Profile dialog:

1. Create an email with the required attachment(s) and click **Send**. The Protect Profile dialog is displayed.

2. Select the profile you want to apply to your attachments and click **Send**.

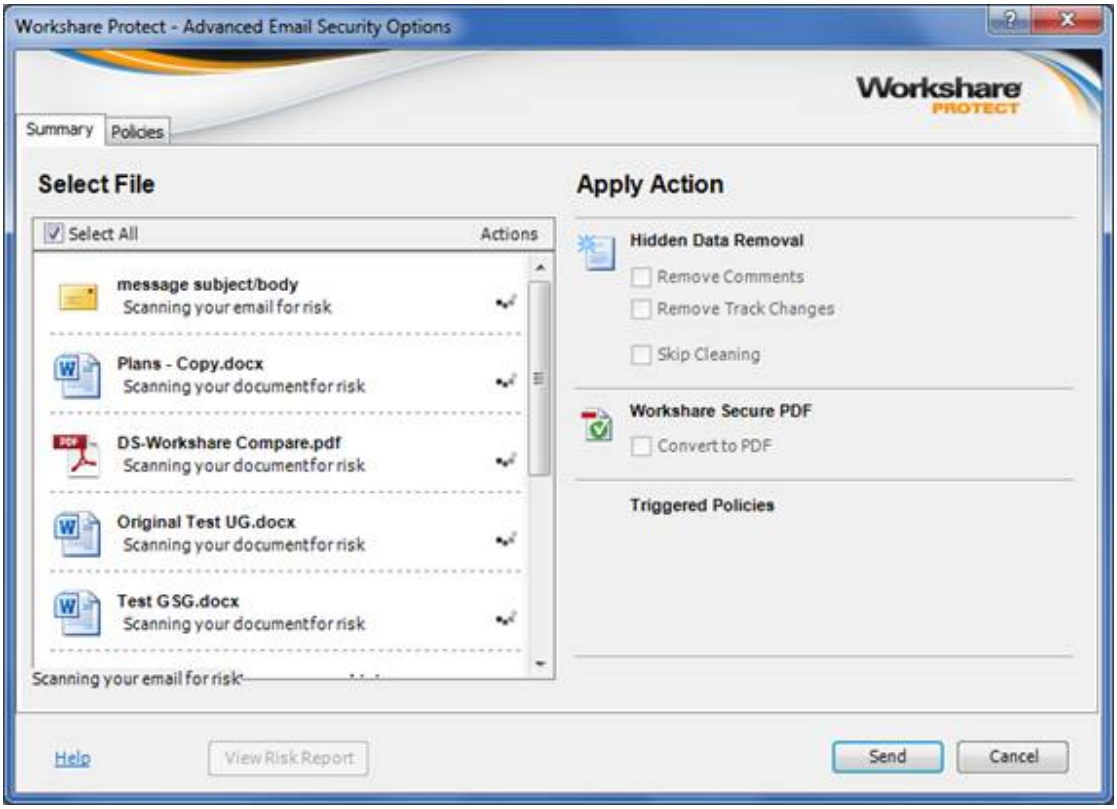
If you want to send your email without Workshare Protect processing the attachments, click the arrow on the **Send** button and select **Send without processing**.

If you want to access *the Email Security* dialog and specify personal settings or individual settings for each attachment, click the **Advanced Options** link. The *Email Security* dialog is displayed with all options enabled.

How to:

Send secure emails using the Email Security dialog:

Create a new email with the required attachment(s) and click **Send**. Workshare Protect alerts you to any breaches of security policies by displaying the *Email Security* dialog.



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. The options available to you depend on 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.
- **Alert Action**: This action alerts you to content risk contained within your email, although you are still able to send the email.
- **Clean/Lightspeed Clean Action**: This action cleans the email and attached documents before sending the email.
- **PDF Action**: This action converts attached documents to PDF before sending the email.
- **Zip Action**: This action zips attached documents before sending the email.

In order to discover more information about what caused a breach of 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.

Refer to *Chapter 9: Protecting Email Attachments* in the *User Guide* for more information.

Clean Hidden Data

Workshare Protect can remove hidden data from open documents as well as clean hidden data from email attachments before they are sent, thus ensuring that the recipient only has knowledge of what the sender intended. Hidden data can include: track changes, comments, footnotes, author's names, server names, authoring trails.

How to:

Clean hidden data from your open documents:

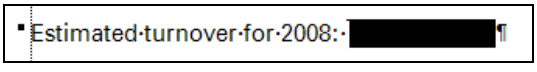
1. Open the document you wish to clean.
2. Click **Content Risk** in the Workshare Panel. Workshare Protect checks the document for content risk. This process may take a few moments if your document is large or if it contains large amounts of content risk. Once the discovery process is complete, the Content Risk page of the Workshare Panel is displayed showing a summary of the content risk found. The content risk found is divided into high risk, medium risk and low risk.
3. To display details of the content risk found, click ▸ to the left of the content risk type.
4. Click **Remove**. The *Advanced Options* dialog is displayed.
5. Select the hidden data you want to remove and click **OK**.

Refer to *Chapter 8: Managing Content Risk in Documents* in the *User Guide* for more information.

How to:

Manually redact selected text:

1. Select the word, sentence or other data that you want to black out.
2. Right-click the selection and select **Redact Text**. The selected text is blacked out.



Create PDFs

Workshare Protect enables you to convert your documents to PDF files. This is useful if you want to maintain a file in its current format, as PDF documents cannot be edited as easily as Microsoft Office documents.

You can also use Workshare Protect to convert PDF files to Microsoft Word files. This is useful if you want to edit the document, as PDF documents cannot be edited as easily as Microsoft Word documents.

How to:

Create PDFs:

1. Open the document you want to convert to PDF.
2. Click **Convert to PDF** in the Workshare Panel. The *Create PDF* dialog is displayed.

3. Click **PDF Security Options**. You can clean hidden data from the document before converting it to PDF as well as increase the security of the document by prohibiting printing, modification of text, text or graphics being copied, comments being added or all of the above. Enter a password to password-protect these settings. Click **OK**.
4. To convert selected pages to PDF, click the **Pages** radio button and enter a specific page range.
5. Click **OK**.
6. The *Save As* dialog is displayed. Enter the required file name and select the appropriate folder. Click **Save**.

Refer to *Chapter 11: Converting to PDF* in the *User Guide* for more information.

How to:

Create PDFs and send by email:

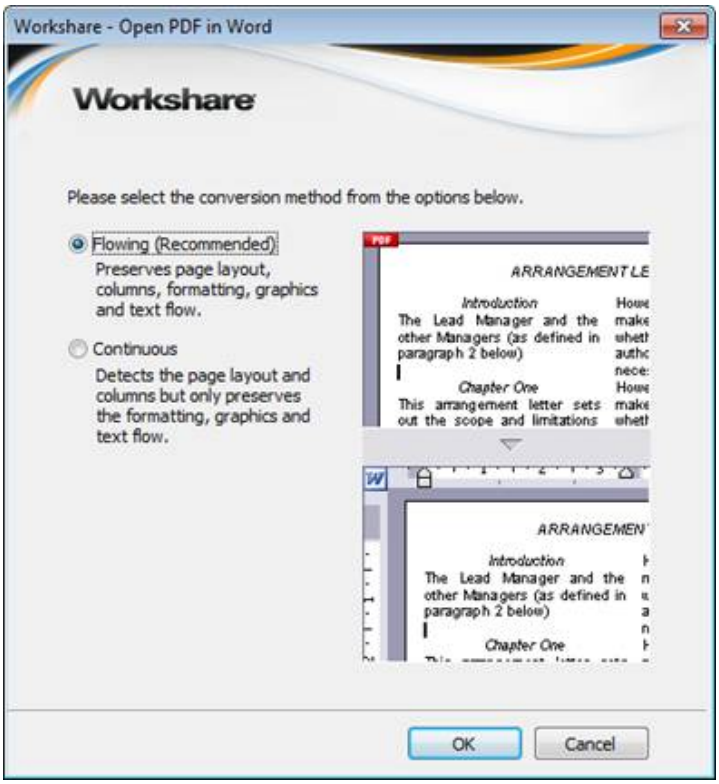
1. Open the document you wish to convert to PDF and send and click **PDF Email** in the *Workshare* tab (**Secure** group) (MS Office 2007) or **Convert to PDF and Email** in the Workshare toolbar (MS Office 2003). The *Create PDF* dialog is displayed.
2. Enter the desired security settings and the page range and click **OK**. The *Save As* dialog is displayed.
3. Enter the required filename and select the appropriate folder and click **Save**. A new email message window opens with the PDF attached.
4. Enter the desired recipients, write your message and click **Send**.

Refer to *Chapter 11: Converting to PDF* in the *User Guide* for more information.

How to:

Convert PDFs to DOC format:

1. Right-click the closed PDF file on your desktop or DMS and select **Open in Word with Workshare** from the menu, or from Microsoft Word, select **Open** from the *File* menu or Office Button menu and browse to the PDF file and click **Open**. The *Workshare PDF to Word Document Converter* dialog is displayed.



2. Select a conversion method according to how much of the formatting and layout you want to preserve and click **OK**. The PDF document is converted to DOC format and is opened in Microsoft Word.

You must save the document. Refer to *Chapter 11: Converting to PDF* in the *User Guide* for more information.

Protect Confidential Documents

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

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

How to:

Classify documents:

1. Open the document you want to classify.
2. Click **Classify** in the Workshare Panel. The Document Classification page is displayed.
3. Select the classification level you require from the dropdown list.
4. If you want to password-protect the classification level, click **Specify a password** in the **Select Password Protection** area.
5. Enter the password twice to set and confirm the password and click **OK**. This means that only those who know the password can change the classification level of the document. Click **Apply**.
6. Save the document. The open document is now restricted according to the selected classification level.

Refer to *Chapter 10: Controlling Documents* in the *User Guide* for more information.