Workshare Protect 8

Getting Started Guide

Version 1.0 | October 2013

Company Information

Workshare Protect Getting Started Guide

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

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

Workshare Website: www.workshare.com

Trademarks

Trademarked names appear throughout this guide as well as on other parts of the Workshare Protect CD. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

Disclaimers

The authors/publishers of the Workshare Protect Getting Started Guide and associated Help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated Help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective Help material possible.

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

Copyright

Table of Contents

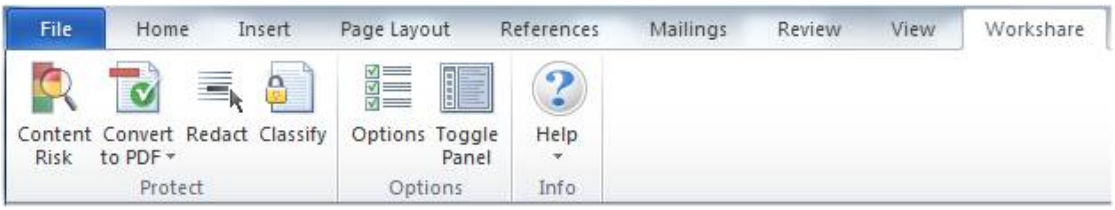
Introducing Workshare Protect

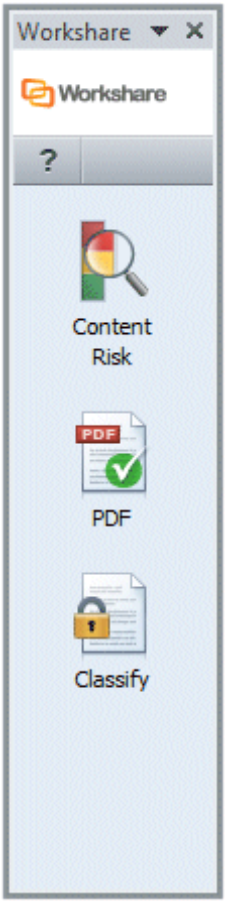
Workshare Protect is seamlessly integrated with Microsoft Office and automatically enforces company security policy at end-user workstations. Rather than simply block information flow, Workshare Protect warns and educates users in real-time about sensitive information and, if authorized, lets users decide 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
- **Storage of Attachments in Workshare Online**
  - Uploading attachments to Workshare Online and sending recipients links to the documents
  - Frees users from having to send attachments by email
  - Facilitating the sharing of files outside of email
- **Tamper-Proof PDF Creation**
  - Converting any document to Workshare's secure PDF from any application
  - Ensuring flexible publishing and complete PDF security options
  - Enforcing automatic conversion of documents to secure PDF before they can be emailed
- **Stopping of Violations in Real Time**
  - Enabling users to fix potential problems with manual redaction options
  - Password-protecting documents or restricting them from being sent externally, or at all.
- **Content Protection and Control**
  - Content analysis and data leak prevention
  - Automatically stopping leaks of intellectual property at their origin
  - Keeping data safe and secure from embarrassing public disclosures
  - Monitoring all communications at the client level
  - Providing alerts for data in use, at rest, and in motion—even when disconnected from the network

Note: *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 Protect integrates into your existing Microsoft Office environment. To this end, there is no independently accessed user interface for Workshare Protect - the user interface is accessed from within Microsoft Word, Excel, PowerPoint or Outlook and is available from all documents.

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

You can show/hide the Workshare Panel by clicking **Toggle Panel** in the *Workshare* tab.

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

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

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

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:

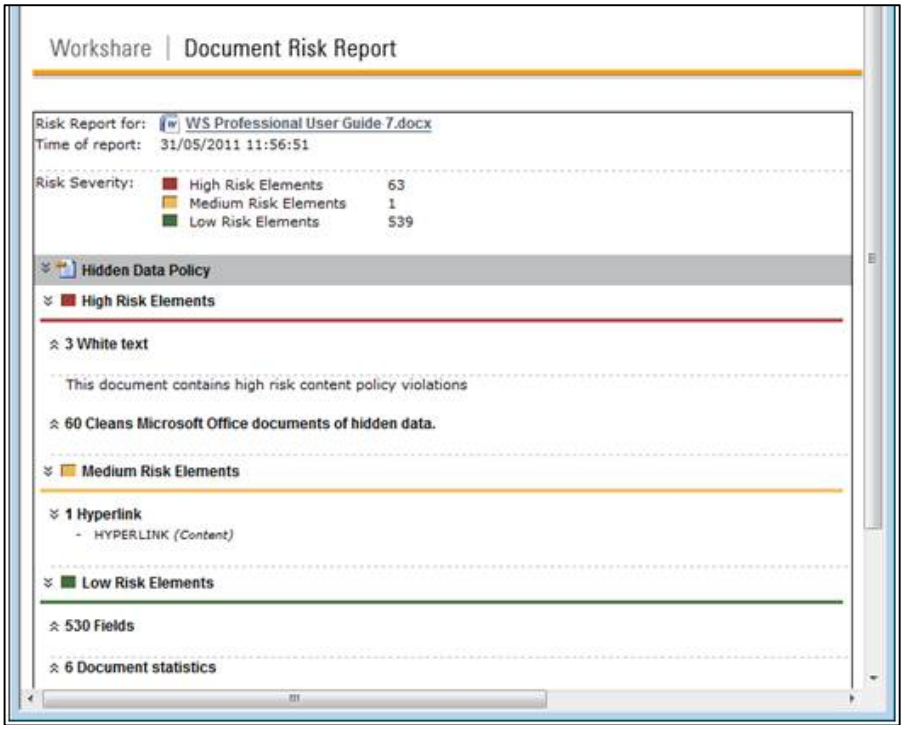
- **Content Risk Reports**: Workshare Protect integrates with Microsoft Office providing an option to display a comprehensive report of all the content risk in a document while it is open in Microsoft Office.
- **Email Protection**: Workshare Protect prevents users from accidentally emailing confidential 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, convert attachments to PDF or PDF/A or compress multiple attachments into a single zip file. Additionally, Workshare Protect can send attachments to a secure location and send recipients a link to that location. 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 experience one of the following three options:

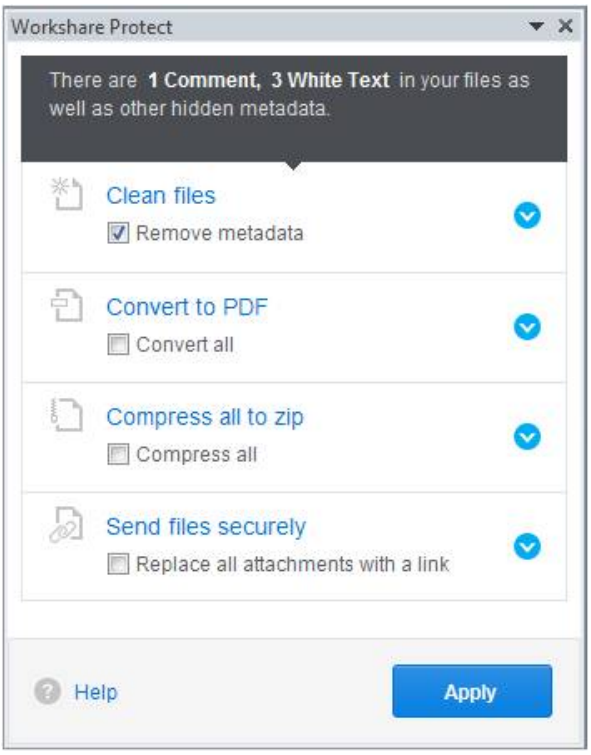
- Interactive Protect panel
- Protect Profile dialog
- Email Security dialog

Interactive Protect Panel

How to:

Send secure emails using the Interactive Protect panel:

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



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

Click the arrow to extend each section to set specific settings. After selecting the required options, 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.

Protect Profile 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**.

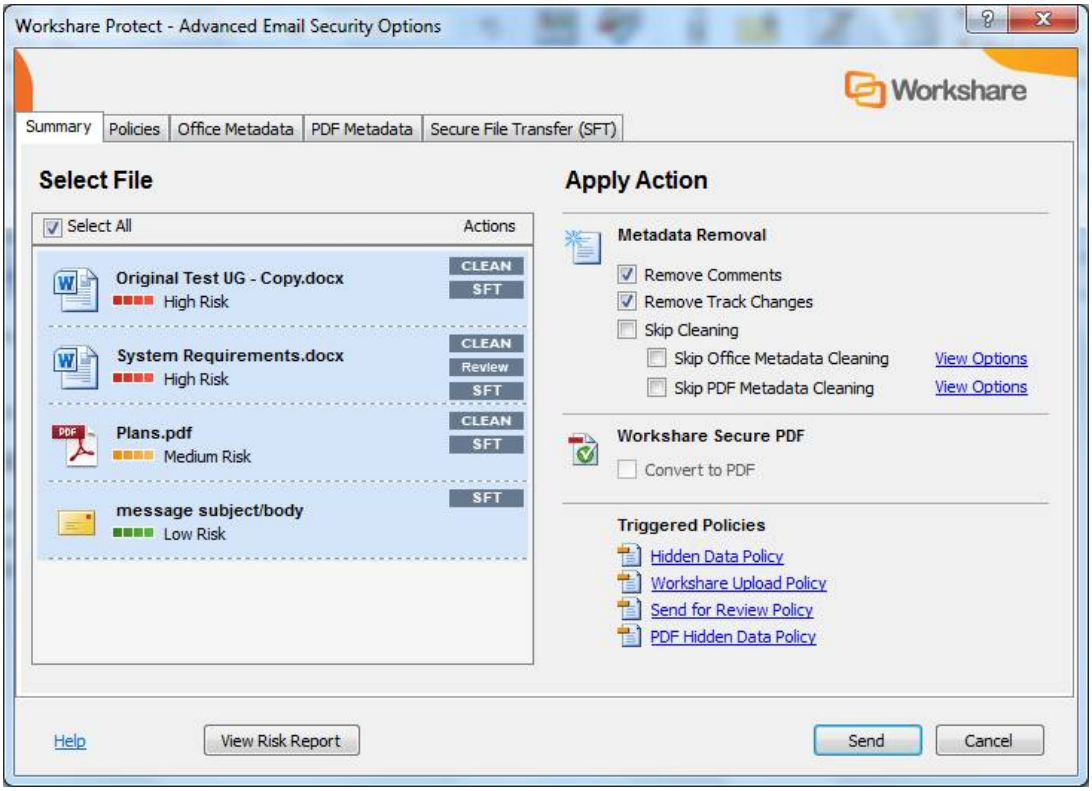
If you want to access *the Email Security* dialog and specify personal settings or individual settings for each attachment, click the **Advanced Options** link. The *Email Security* dialog is displayed with all options enabled.

Email Security Dialog

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:

- **Block Action**: Blocks your attempts to send the email until the offending information is removed.
- **Alert Action**: Alerts you to content risk contained within your email, although you are still able to send the email.
- **Clean/Lightspeed Clean Action**: Cleans the email and attached documents before sending the email.
- **PDF Action**: Converts attached documents to PDF before sending the email.
- **Zip Action**: Compresses attached documents before sending the email.
- **Secure File Transfer**: Uploads attachments to Workshare Online and sends recipients a link to the attachments in Workshare.

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 4: Protecting Email Attachments* in the *User Guide* for more information.

Receiving Links

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

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

Sending Large Files

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

When you try and add a file with a size over the specified limit, Microsoft Outlook may display a message saying that the attachment size exceeds the allowable limit. In this case, you can use the **Add Large Attachment** button to access the Send Link functionality.

To send large files:

1. Open a new email message window and click **Add Large Attachment**.
2. Browse to the large file you want to attach and click **Open**. The attachment displayed in the message appears small because it is only a pointer to the large file.
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 attached large file is uploaded to a folder in Workshare. The name of the folder is whatever is entered into the **Subject** field of the email followed by the date and time. This folder appears in your Sent Items folder in My Files and Folders in Workshare. The recipient receives an email notifying them that file has been uploaded to Workshare and providing a link to the file.

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:

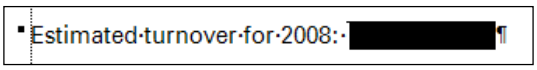
1. Open the document you wish to clean.
2. Click **Content Risk** in the Workshare Panel. Workshare Protect checks the document for content risk. This process may take a few moments if your document is large or if it contains large amounts of content risk. Once the discovery process is complete, the 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 3: 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

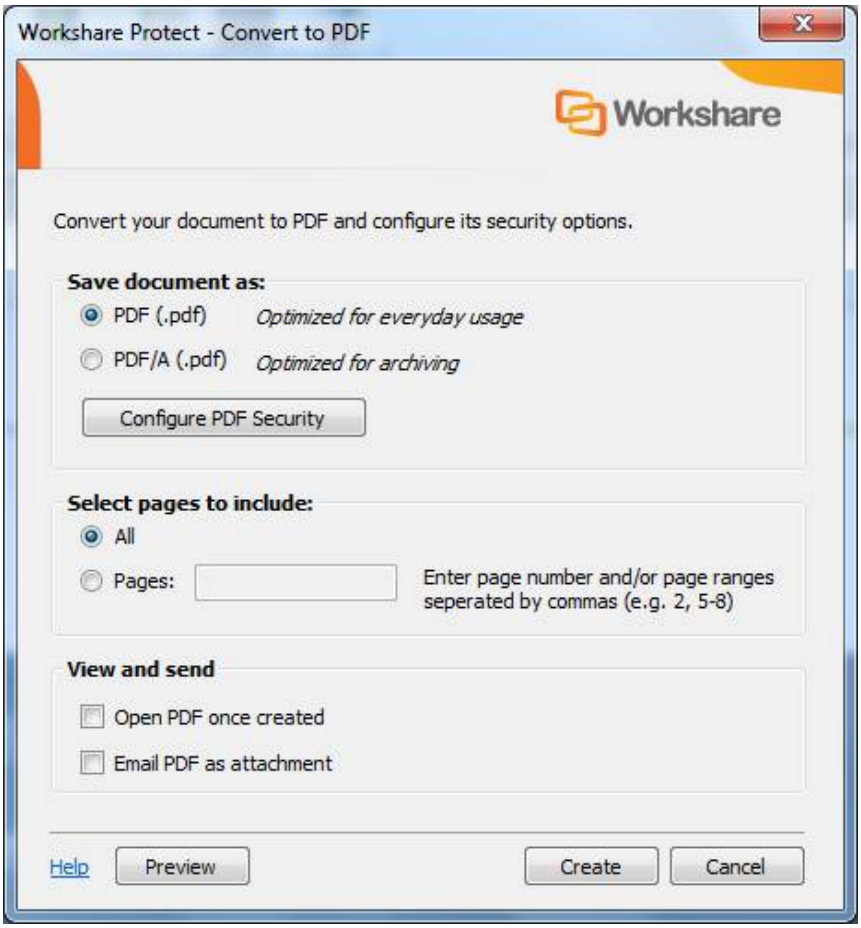
Workshare Protect creates the most secure PDF files available from any application. You can quickly and easily convert open and closed Microsoft Office documents into PDF or PDF/A. You can also enforce PDF creation on email attachments leaving your organization. When sending documents for review, you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

Workshare Professional provides accurate conversion of PDF files to Microsoft Word files (PDF to DOC/DOCX format) preserving document formatting and page layout. This Workshare Professional functionality is available from within Microsoft Word and by right-clicking closed PDF files on your desktop.

How to:

Create PDFs:

1. With your document open in Microsoft Word, Excel or PowerPoint, click **Convert to PDF**.



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

3. Click **Configure PDF Security** to set PDF security options and remove metadata. You can clean hidden data from the document before converting it to PDF as well as increase the security of the document by preventing 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.
3. Select the **Open PDF once created** checkbox if you want the PDF to be opened once it has been created.
4. Select the **Email PDF as attachment** checkbox if you want the PDF to be attached to an email once it has been created.
5. If required, click **Preview** to view the document as a PDF.
6. Click **Create**. The *Save As* dialog is displayed:
7. 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.

Refer to *Chapter 6: 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 whether externally or internally, it will be blocked.
- **External Restriction**: The document is restricted and can only be distributed internally within your organization. Use this status if you are collaborating on a document with colleagues, but the document is not yet ready for client review.
- **Full Restriction**: The document is restricted and cannot be distributed via email. Use this status if you are working on a document yourself and do not want it distributed.

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 5: Controlling Documents* in the *User Guide* for more information.