

What Is Content Risk?

The term **Content Risk** refers to a variety of types of information that can be contained in Microsoft Word, Excel, or PowerPoint documents. Content Risk includes hidden data, such as tracked changes and comments, and visible content in documents that, if exposed, could violate your firm's privacy, intellectual property, or financial disclosure policies. Examples of Content Risk include social security numbers, company financials and employee and customer information.

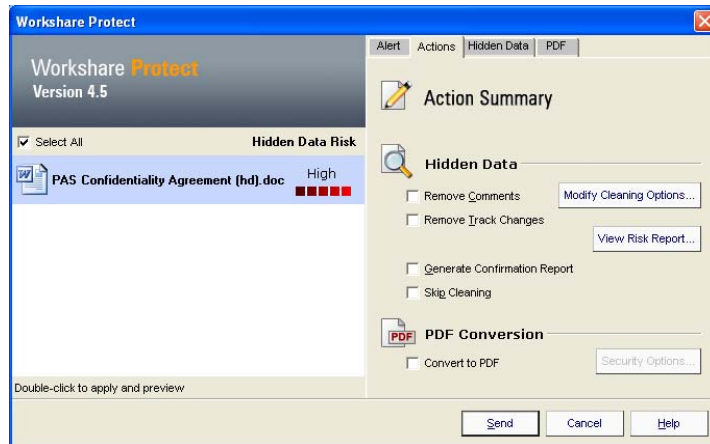
Workshare Protect alerts users to the presence of Content Risk, whether or not the information is hidden or visible, and can also remove hidden data before the document leaves the firm via email.



Hidden data, such as the tracked changes and comment shown above, can include information that should not be sent outside the firm.

Using Workshare Protect

Each time you send an email with an attachment outside the firm, a Workshare Protect dialog box allows you to remove hidden data and safely send the document. You are also alerted to any content that might be in violation your firm's policies.



To Remove Hidden Data from an Email Attachment

1. Create an email message with an attachment that is addressed to a recipient outside the firm.
2. Click **Send**. A Workshare Protect dialog box is displayed.
3. On the **Actions** tab, make selections in the **Hidden Data** area.

To do this...	Do this...
Clean track changes and/or comments as well as all other hidden types	Check the Remove Track Changes and/or Remove Comments box and leave the Skip Cleaning box unchecked.
Do not clean track changes or comments, but clean all other hidden data types	Leave the Remove Track Changes and Remove Comments boxes as well as the Skip Cleaning box unchecked.
Do not clean any hidden data in the document	Check the Skip cleaning box (not recommended).

4. Click **Send**. Workshare Protect cleans the document according to your selections, and sends it. The cleaned file can be found in sent email.

Alerting on Content Risk

Workshare Protect alerts you if the document you are sending outside the firm contains Content Risk that, while not hidden, could be compromising. Examples of this type of content include social security numbers, credit card numbers and profanity.

Your firm's IT administrators can customize this functionality to recognize any words or phrases that might be compromising.

To View Content Risk

1. Create an email message with an attachment that is addressed to a recipient outside the firm.
2. Click **Send**. A Workshare Protect dialog box is displayed.
3. If the document contains high risk content, the **Alert** tab of the Workshare Protect dialog box is displayed, notifying you of the possible policy violation.



4. Cancel the Alert, remove the document from the email message, and remove or replace high risk content.
or
Click the **Next** button to display all tabs on the Workshare Protect dialog box. The Content Risk is not removed.

Caution: The Content Risk Alert *does not* automatically remove potential violations (social security numbers, profanity, etc.) when the document is sent. If you wish to remove this type of Content Risk, you must manually make edits within the document before sending it .

Sending PDF Files

Workshare Protect email integration also lets you convert documents to PDF "on the fly" in outgoing email attachments.

To Convert an Email Attachment to PDF


1. Create an email message with an attachment that is addressed to a recipient outside the firm.
2. Click **Send**. A Workshare Protect dialog box is displayed.
3. On the **Actions** tab, in the **PDF** area, check the **Convert to PDF** box.
4. Switch to the **PDF** tab, or click the [Details...](#) link, to change your security options.
5. (Optional) You may secure the document by choosing to **Prohibit Printing**, **Prohibit modification of text**, **Prohibit text or graphics being copied**, and/or **Prohibit comments being added**. You may also password-protect the document.
6. Click the **Send** button. The PDF file is sent and can be found in your sent email.

Caution: If the Word document contains tracked changes or comments, these may be displayed in the PDF file, too. It is recommended that you select to remove this hidden data when you convert to PDF.

Using Advanced Content Risk Tools

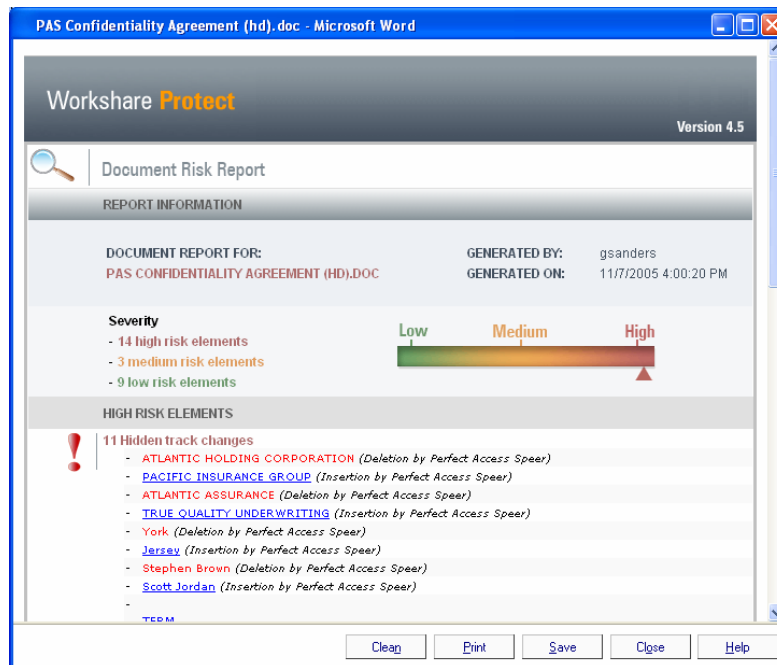
Although Workshare Protect Content Risk protection is activated every time you send an email attachment externally, Workshare Protect also contains advanced tools available from within Word for analyzing and cleaning a document.

To Check a Document for Content Risk

1. Open the document you want to check for Content Risk.
2. Click the **Discover Content Risk**  button on the toolbar.

or
Select **File/Discover Content Risk**.


A Workshare Protect Document Risk Report is displayed with information about any Content Risk in the document. This is displayed as High Risk, Medium Risk and Low Risk.

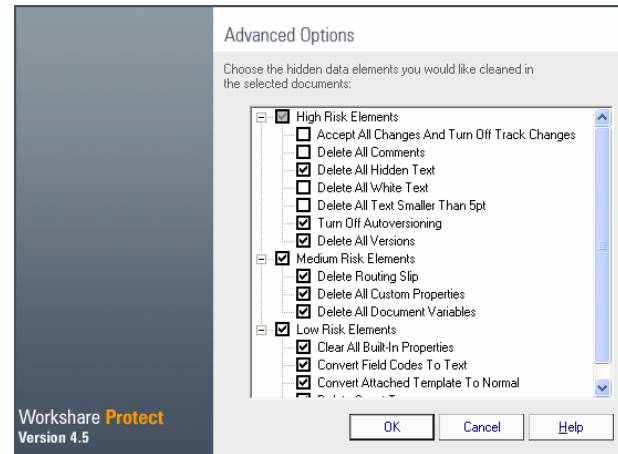


3. (Optional) Click the  and/or  buttons to print and/or save the Document Risk Report.

To Clean the Working Copy of a Document

Running content risk cleaning from the Document Risk Report dialog allows you to clean hidden data from any open Word document.

1. With the Document Risk Report displayed, click the  button. The Advanced Options dialog opens.



2. Select the cleaning level (**High Risk Elements**, **Medium Risk Elements**, or **Low Risk Elements**) or you may select individual actions by marking or clearing the appropriate check boxes.
3. Click **OK**.
4. When cleaning finishes running, the Document Risk Report refreshes and displays any remaining hidden data.

Caution: Cleaning the working copy of a document *does not* automatically remove potential violations (social security numbers, profanity, etc.). If you wish to remove this type of Content Risk, you must manually make edits within the document before sending it.

WORKSHARE PROTECT 4.5

DISCOVERING CONTENT RISK AND SENDING FILES AS PDF

Find help on these topics:

WHAT IS CONTENT RISK?

USING WORKSHARE PROTECT

To Remove Hidden Data from an Email Attachment

ALERTING ON CONTENT RISK

To View Content Risk

SENDING PDF FILES

To Convert an Email Attachment to PDF

USING ADVANCED CONTENT RISK TOOLS

To Check a Document for Content Risk
To Clean the Working Copy of a Document