

CONTENT RISK IN DOCUMENTS

What is Content Risk?

Workshare Professional provides comprehensive content risk protection enabling the discovery and removal of hidden sensitive data as well visible sensitive data. Hidden data may include information such as track changes, author's name, server names, keywords, routing slips and authoring trails. Visible sensitive data may include financial information, social security numbers, credit card numbers or profanity. Content risk is defined in security policies.

Workshare Professional enables the discovery of content risk in the following ways:

- **Content Risk Reports:** Workshare Professional 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 Word, Excel and PowerPoint. Content risk is displayed according to its risk level (high, medium, low). Once discovered, it can be cleaned.
- **Email Protection:** Workshare Professional prevents users from accidentally emailing confidential information by alerting users before the email is sent when an email or its attachment breaches security policies.
- **Real-Time Alerts:** When open Microsoft Office documents trigger a breach of a security policy with an Active Task Bar action defined, a real-time policy alert is displayed in the bottom right of the screen notifying the user of the policy breach. When open Microsoft Office documents trigger a breach of a security policy with a Smart Tag action defined, a smart tag (a purple dotted line beneath the text) notifies the user of the policy breach.

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

Content Risk Reports

Workshare Professional integrates with Microsoft Office to provide an option to discover and view content risk in a document. You can also display a comprehensive report of all the content risk in a document.

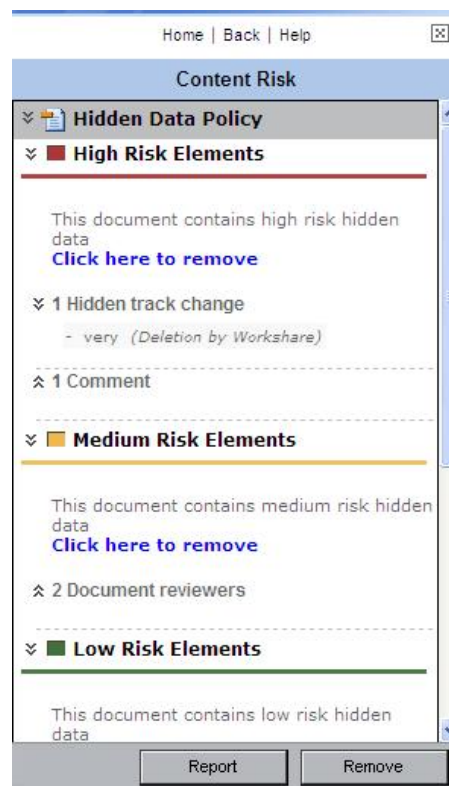
To discover content risk in your document:


Open your document in Microsoft Word and click Content Risk in the Home page of the Workshare Panel.

Workshare Professional 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.



Note: In Microsoft Excel and PowerPoint, a summary of the content risk is shown in the Document Risk Report.



The content risk found is divided into high risk, medium risk and low risk (according to the risk level specified in the policy). To display details of the content risk found, click  to the left of the content risk type.

WORKSHARE PROFESSIONAL QUICK REFERENCE

To remove hidden data:

1. In Microsoft Word, click Remove in the Content Risk page. In Microsoft Excel or PowerPoint, click Remove in the Document Risk Report. The *Advanced Options* dialog box is displayed showing a complete list of hidden data that can be removed, reset or converted.
2. Select the hidden data you want to remove and click OK. The selected hidden data is removed from the document.

Real Time Alerts

As you are working on a document, Workshare Professional checks the document content to see if it breaches any security policies. For example, you could enter sensitive financial information.

A security policy defines the conditions that must exist in order for Workshare Professional to detect content risk and the actions that should be taken when the conditions are met (i.e. content risk is found). In the case of open Microsoft Office documents, the possible actions are as follows:

- **Active Task Bar Action:** Real-time policy alerts appear in the bottom right of the screen notifying you of the policies breached by the open Microsoft Office document.
- **Smart Tag Action:** Workshare Professional expands the types of data recognized by Microsoft Word so that policy breaches in a document are indicated by the use of a smart tag.

Manual Redaction

Workshare Professional provides the functionality for you to manually redact/black out selected content in Microsoft Word (DOC and DOCX) documents. Redacting text is to black out the text so that it is no longer discernible.

The functionality is available from a right-click menu and also from the Workshare tab (MS Word 2007) and Workshare Professional toolbar (MS Word 2003/XP).

Redacting text actually replaces the text with "pipes" (| | | | |) on a black background. Once you make redactions in your document and save it, the redacted text cannot be restored (apart from the immediate possibilities of the Undo action).

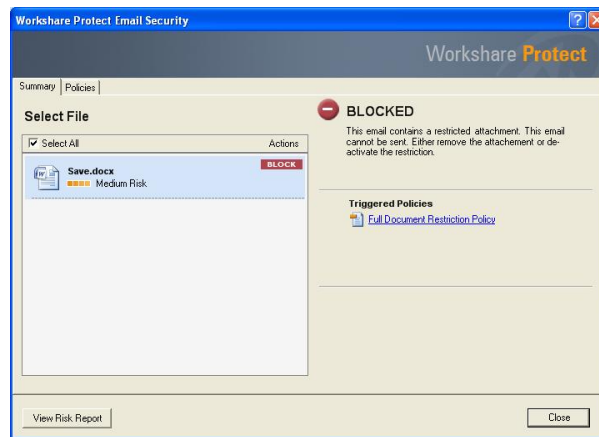
Email Protection

Every time you send an email, Workshare Professional checks the email content and any attachments to see if they breach any security policies. For example, an attached document could contain hidden data that should not be sent to external parties. Or, an email could contain sensitive financial information that should not be distributed by email at all.

To send secure emails:

Create a new email, attach the required document(s) and click Send.

Workshare Professional alerts you to any breaches of security policies by displaying the *Email Security* dialog.



This dialog alerts you to any breaches of security policies triggered by your email or its attachments.

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.



Note: The availability of checkboxes and options may appear differently depending on your organization's security policies.

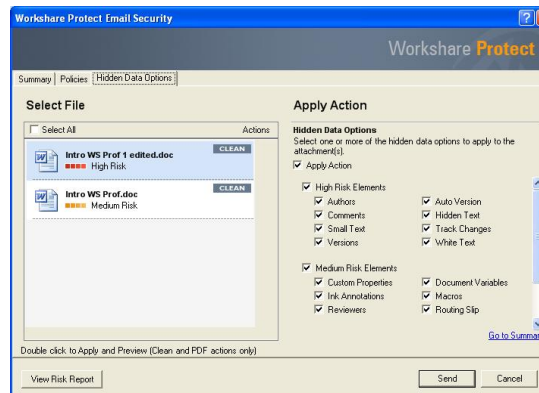
The options available to you depend on the action specified for a policy breach. The different actions are as follows:

- **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 Action/Lightspeed Clean Action:** This action cleans the email and attached documents before sending the email. A Lightspeed Clean is faster than a regular Clean.
- **PDF Action:** This action converts attached documents to PDF before sending the email.
- **Zip Action:** This action zips attached documents before sending the email.

To clean hidden data from email attachments:

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 in the Apply Action area.

1. Select the attachment in the Select File list and click Go to Hidden Data Options in the Apply Action area or select the Hidden Data Options tab.



2. Select the hidden data that you want to remove by selecting or deselecting the relevant checkboxes.
3. Repeat step 2 for additional attachments to specify individual clean settings for each attachment or select Select All.

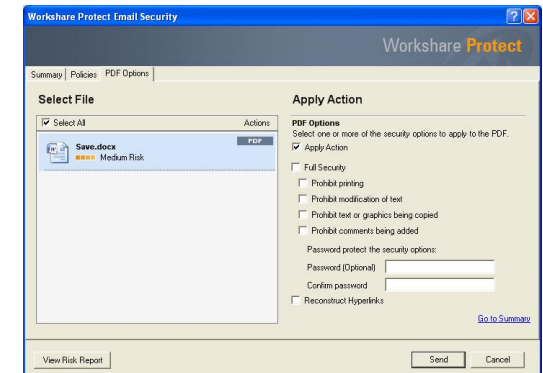
4. Click Send to send the email.

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

To convert attachments 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.

1. Select the attachment in the Select File list and click Go to PDF Security in the Apply Action area or select the PDF Options tab.



2. Select one or more of the security options individually or select the Full Security checkbox to select them all. The security options include preventing recipients from printing, editing, copying from or adding comments to the PDF attachment.
3. If required, set a password for access to the PDF security settings by entering the password twice in the relevant fields.
4. If required, select the Reconstruct Hyperlinks checkbox to preserve standard URL and bookmark hyperlinks
5. Repeat steps 2 to 4 for additional attachments to specify individual PDF settings for each attachment or select Select All.
6. Click Send to send the email.

Workshare Professional converts the attachments to PDF and applies your settings before sending the email.