Workshare Protect Server

Metadata Removal

Workshare Protect Server 3.11 | August 2018

Table of Contents

Chapter 1: Introducing Workshare Protect Server

This chapter introduces Workshare Protect Server, 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 Server?**, page 6, introduces Protect Server.
- **Workshare Protect Server Functionality**, page 6, describes the different functionality available with Protect Server.

What is Workshare Protect Server?

Workshare Protect Server provides server-side metadata cleaning and document processing. Protect Server processes all emails passing through the corporate mail server, including those that originate from webmail and mobile mail clients. In corporate email scenarios, email is always routed through the corporate email server - and consequently Protect Server - ensuring complete protection. By locating this processing effort on the server, email send performance on the originating device is not impacted, and users are not affected.

Protect Server is a mail gateway that removes metadata from Microsoft Office attachments (Word, Excel and PowerPoint) as well as PDF attachments. It can also automatically convert Microsoft Office attachments to PDF. A web application - the Workshare Protect Server web console – is provided to enable administrators to configure which metadata elements to remove and view a history of what was previously removed.

Additionally, Protect Server can include the Policy Editor which provides a new policy framework to determine whether an email should be sent or bounced. It provides for control at the matter level through policies that associate email whitelists with matter-IDs.

Workshare Protect Server Functionality

Workshare Protect Server can secure attachments before they are sent by cleaning them of metadata or converting to PDF. Additionally, Protect Server can block emails and prevent them from being sent at all. An overview of the functionality is provided in the following sections.

Securing email attachments

Protect Server processes emails leaving an organization according to the profile applied to the email. This processing could be cleaning the attachments by removing metadata from them or converting the attachments to PDF, or both.

Where emails are sent to both internal and external recipients and the Workshare Protect Routing Agent is **not** installed, the internal recipient will receive the unprocessed document and the external recipient will receive a processed version. When the Protect Routing Agent **is** installed, both internal recipients and external recipients will receive a processed version.

Protect Server processes Microsoft Office and PDF attachments. The following file formats can be processed:

File format	Cleans	Converts to PDF or PDF/A
Microsoft Word 97 or later (DOC, DOT, DOCX, DOTX, DOCM, DOTM)	✓	✓
Microsoft Excel 97 or later (XLS, XLT, XLSX, XLTX)	✓	✓
Microsoft PowerPoint 97 or later (PPT, POT, PPTX, POTX)	✓	✓
RTF	✓	✓
Word 2003 XML	✓	✓
Open Document Text (both ODT 1.1 and 1.2 are cleaned, but files saved in ODT 1.1)	✓	✓
PDF	✓	✗

Protect Server processes the following types of attachments:

- Password-protected attachments (when the Workshare Protect Portal is installed).

> ***Note**: Protect Server does not process password-protected PowerPoint files.*

- The contents of archive (ZIP) attachments.
- Attachments of embedded emails.
- Attachments to meeting requests and other Microsoft Exchange-specific features, such as polls and forms.

> ***Note**: Protect Server does not process digitally signed documents or corrupt documents and does not check the attachments of digitally signed emails.*

Workshare Protect Routing Agent

With the installation of the Protect Routing Agent, Protect Server processes attachments of emails that are sent to both internal and external recipients. When an email has a relevant attachment and includes both external and internal recipients, the Protect Routing Agent will ensure that both the internal recipient and the external recipient receive the same processed version of the attachment.

The installation and setup of the Protect Routing Agent is described in the *Workshare Protect Routing Agent Admin Guide*.

Profiles determine cleaning and conversion

Profiles specify what metadata to remove from an email attachment and whether to convert the attachment to PDF. Every profile has an email address and this is how Protect Server determines which profile to apply to any given email. When a sender adds the email address of a profile as a recipient in an email then this profile will be used to process the email.

When a sender does not specify a profile email address in an email, the following occurs:

- If you have enabled the Active Directory cache feature, then Protect Server will look to see what AD group the sender belongs to and apply whichever profile you have defined for that group. If no profile has been defined for the group, then Protect Server will apply whichever profile you defined as the Default profile.
- If you have **not** enabled the Active Directory cache feature, then Protect Server will apply whichever profile you have defined as the Default profile.

If the sender specifies more than one profile email address in an email, then Protect Server will apply whichever profile you have defined as the Fallback profile.

Users allocated an Administrator role can create and manage multiple metadata cleaning/PDF conversion profiles. Users allocated a Business or User role can only view profiles. They cannot create new profiles or modify or delete existing profiles.

Rule-based email blocking

Protect Server can prevent emails from being sent, based on business rules. The decision to block emails is driven by policies configured in the Protect Server Policy Editor. The Policy Editor provides for control at the matter level through policies that associate email groups with client engagements.

Policies determine access

You can set a policy that tells Protect Server to look for specific custom properties in the email attachments together with specific email addresses. If found, the email will be bounced.

The Policy Editor supports both whitelisting and blacklisting with policies that ensure access to certain information is to pre-approved recipients only as well as policies that ensure certain documents are never sent to untrustworthy recipients.

This granular approach to policies ensures confidential files pertaining to confidential matters are not accidentally sent to the wrong people.

This functionality can be enabled during or after installation. Configuring policies is described in the *Workshare Protect Server Email Data Loss Protection guide*.

Additional functionality

Additional functionality can be configured on the Protect Server web console.

- **Clean reports for senders**

  Senders receive a clean receipt email with a Clean Report PDF attached providing details of the exact metadata cleaned from the document. The clean receipt email can also include the original email and the processed attachments. Administrators configure clean receipts on the Protect Server web console.

- **Bouncing emails**

  Protect Server can be configured to prevent emails with attachments that include comments or track changes or that cannot be processed from being delivered. There are several reasons why Protect Server may not be able to process an attachment. For example, the attachment may be corrupt or digitally signed. When Protect Server is configured this way, it bounces the email back to the sender with a non-delivery report. Administrators configure which emails to bounce on the Protect Server web console.

- **Preview functionality for senders**

  Protect Server provides previews of the cleaned/converted attachments to the sender. The sender can request a preview of what the processed attachments will look like before sending them to the recipients. This is done by sending an email to a profile email address only. Protect Server will treat such an email as a preview request and send the processed attachments back to the sender.

- **Synchronization**

  You can configure synchronization so that where any email attachment is processed by Protect Server, the original copy of the email found in the sender’s “Sent Items” folder will be updated with the processed attachments. This update occurs for email destined for external recipients only as well as emails destined for both internal and external recipients.

  Additionally, to ensure that internal recipients always have access to the same version of attachments that are received by external recipients, where emails are sent internally and externally, the internal recipients can receive a clean receipt with the processed attachment included.

Web console for configuration

The functionality available in the Protect Server web console depends on the type of user:

- Users allocated an **Administrator** role can do the following:
  - View information about the performance and current health of Protect Server. For example, whether Protect Server services are up and running, whether the database is connected, whether the Protect Server license is expired and details of any emails queued on Protect Server.
  - Search through all emails processed by Protect Server.
  - Configure profiles.
  - Define policies (when the Policy Editor is enabled)
  - Specify Protect Server configuration settings, such as whether clean reports should be sent, how to override cleaning settings as well as configuring alert settings and email templates.
- Users allocated a **Business** role can do the following:
  - Access detailed statistics on the activities of Protect Server. For example, how many emails were processed using each profile and how many emails were processed in Microsoft Word format.
  - Search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.
  - View profiles configured for Protect Server. They cannot create new profiles or modify or delete existing profiles.
- Users allocated a **User** role can do the following:
  - Search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.
  - View profiles configured for Protect Server. They cannot create new profiles or modify or delete existing profiles.

***Note**: Roles are allocated during installation.*

The web console and configuration of Protect Server is described in the *Workshare Protect Server Installation guide*.

Chapter 2: Configuring Profiles

This chapter describes profiles and how they are used in Workshare Protect Server. It includes the following sections:

- **Introducing Profiles**, page 12, describes profiles and how they work in Protect Server.
- **Exporting and Importing Profiles**, page 15, describes how to export saved profiles as well as import profiles.
- **Creating Profiles**, page 19, describes how to create profiles and specify what type of metadata should be cleaned from email attachments and whether they should be converted to PDF.

This functionality is available for Administrator role users. Business and User role users can view profiles only.

Introducing Profiles

A profile is a collection of metadata and PDF conversion settings – a set of instructions to Workshare Protect Server as to what metadata to remove from an email attachment and whether to convert the attachment to PDF.

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.

Every profile has an email address and this is how Protect Server determines which profile to apply to any given email. When a user adds the email address of a profile as a recipient in an email then this profile will be used to process the email. When two or more email addresses of profiles are specified as recipients in an email, then whichever profile has been defined as the Fallback profile will be applied.

When the Workshare Protect Server Client is installed, the user can select the profile to apply from the Protect Profile dialog when sending an email. Refer to the *Workshare Protect Server Client Add-on Admin Guide*. This dialog can also be displayed when Workshare Professional or Protect is installed and can be configured to list server profiles. Refer to the *Workshare Configuration Options* guide.

No profile email address

When no email address of a profile has been specified as a recipient in an email and you have enabled the Active Directory cache feature, then Protect Server will look to see what AD group the sender belongs to and apply whichever profile you have defined for that group. If no profile has been defined for the group, then Protect Server will apply whichever profile you defined as the Default profile.

When a sender does not specify a profile email address in an email and you have NOT enabled the Active Directory cache feature, then Protect Server will apply whichever profile you have defined as the Default profile.

Group precedence

When you have enabled the Active Directory cache feature and you indicate in each profile which AD group the profile will apply to, there may be conflict situations and Protect Server will apply profiles according to the following criteria:

- When a sender belongs to a group and also a subgroup within that group, for example “Sales” and “Sales > UK Sales”, Protect Server will apply the profile defined for “Sales > UK Sales” because it is more specific.

- When a sender belongs to more than one group of the same organizational specificity, for example, “Sales” and “Marketing”, Protect Server will apply the profile defined for “Marketing” based on alphabetical order.
- When a user belongs to multiple hierarchical groups, for example, “Sales > UK >London” and “Sales>America”, Protect Server will apply the profile defined for “Sales > UK >London” because it is more specific.

***Note**: These criteria assume profiles have been defined for each group in each case. Where no profile is defined for a particular group, there is no conflict.*

Using the Protect Server web console, you can create new profiles, edit existing profiles and delete profiles. Profiles are listed in the Profiles page.

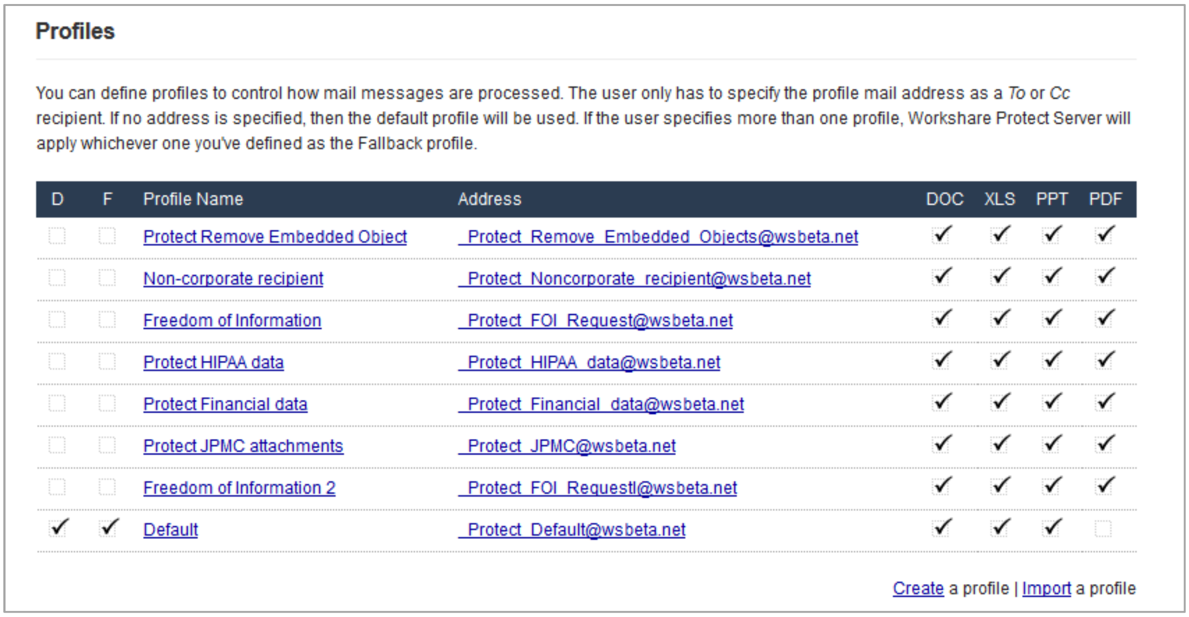
***Note**: The cleaning override email address will always take precedence over any profile email address. So when the cleaning override email address is specified, even if a profile email address is also specified, Protect Server will always skip processing.*

Profiles page

The Profiles page in the Protect Server web console is where you can view the profiles configured on Protect Server. From here, Administrator role users can create new profiles, edit existing profiles and delete profiles.

To display the Profiles page:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Profiles**.



Profiles

You can define profiles to control how mail messages are processed. The user only has to specify the profile mail address as a *To* or *Cc* recipient. If no address is specified, then the default profile will be used. If the user specifies more than one profile, Workshare Protect Server will apply whichever one you've defined as the Fallback profile.

D	F	Profile Name	Address	DOC	XLS	PPT	PDF
□	□	Protect Remove Embedded Object	_Protect_Remove_Embedded_Objects@wsbeta.net	✓	✓	✓	✓
□	□	Non-corporate recipient	_Protect_Noncorporate_recipient@wsbeta.net	✓	✓	✓	✓
□	□	Freedom of Information	_Protect_FOI_Request@wsbeta.net	✓	✓	✓	✓
□	□	Protect HIPAA data	_Protect_HIPAA_data@wsbeta.net	✓	✓	✓	✓
□	□	Protect Financial data	_Protect_Financial_data@wsbeta.net	✓	✓	✓	✓
□	□	Protect JPMC attachments	_Protect_JPMC@wsbeta.net	✓	✓	✓	✓
□	□	Freedom of Information 2	_Protect_FOI_Requestl@wsbeta.net	✓	✓	✓	✓
✓	✓	Default	_Protect_Default@wsbeta.net	✓	✓	✓	□

The Profiles page provides a list of profiles configured on Protect Server. The following information is provided:

D A checkmark in the **D** column indicates which profile is the Default profile - when no profile email address is specified as a recipient in an email, the Default profile is applied.

F A checkmark in the **F** column indicates which profile is the Fallback profile - when two or more profile email addresses are specified as recipients in an email, the Fallback profile is applied.

Profile Name The name specified for the profile.

Address The email address of the profile. This is how Protect Server determines which profile to apply to any given email. When a user adds the email address of a profile as a recipient in an email then this profile will be used to process the email.

Active Directory groups (If configured) The number of Active Directory groups assigned to the profile. When no profile email address is specified as a recipient, this is how Protect Server determines which profile to apply. Protect Server will look to see what AD group the sender belongs to and apply whichever profile has been defined for that group.

DOC A checkmark in the **DOC** column indicates that the profile is configured to process Microsoft Word documents. This could be removing metadata or converting the document to PDF or both.

XLS A checkmark in the **XLS** column indicates that the profile is configured to process Microsoft Excel spreadsheets. This could be removing metadata or converting the spreadsheet to PDF or both.

PPT A checkmark in the **PPT** column indicates that the profile is configured to process Microsoft PowerPoint presentations. This could be removing metadata or converting the presentation to PDF or both.

PDF A checkmark in the **PDF** column indicates that the profile is configured to process PDF files. This could be removing metadata or applying security to the PDF or both.

From the Profiles page, an Administrator role user can click **Create** to create a new profile (refer to Creating Profiles), click **Import** to import a profile (refer to Exporting and Importing Profiles) or click a profile name to view the properties of that profile.

Using the menu on the left, you can view the settings specified for the selected profile with regard to documents, spreadsheets, presentations and PDF files.

Editing profiles

To edit a profile, click the profile name to open it. Click **Edit** and make changes as required.

Deleting profiles

To delete a profile, click the profile name to open it and click **Delete** - you are prompted to confirm the deletion.

If there is only a single profile defined, it cannot be deleted. There must always be a default profile and you cannot delete the default profile without first specifying another profile as the default.

Exporting and Importing Profiles

Exporting a profile enables you to save it as a .wpprofiles file, which can then be imported as required. You can quickly duplicate a detailed policy and make minor modifications or you can ensure consistency by importing the same profile across an environment with multiple Protect Servers. When exporting a profile, the following information is saved:

- Name
- Description
- Email address
- Document metadata rules
- Spreadsheet metadata rules
- Presentation metadata rules
- PDF metadata rules

Whether the profile is "default" or "fallback and the Active Directory cache settings for the profile are not exported.

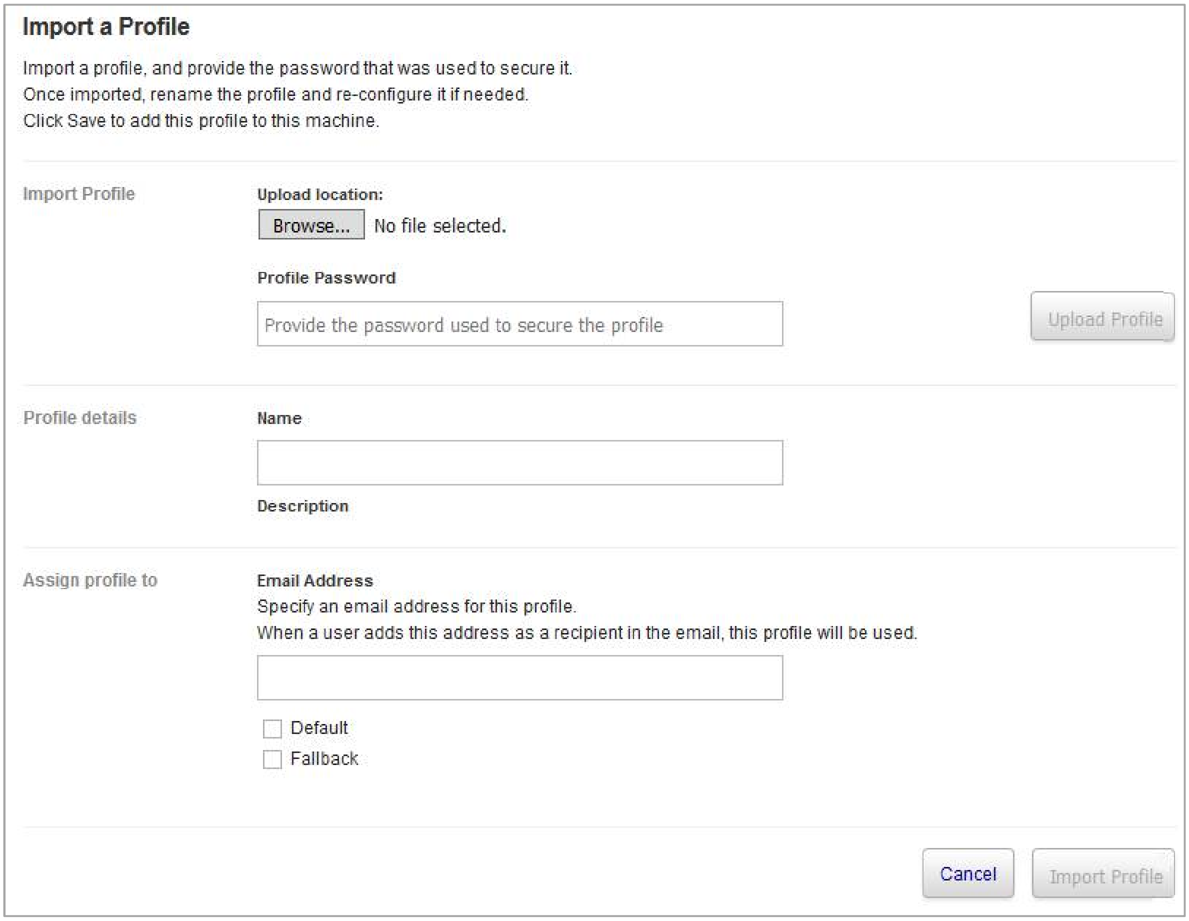
The exported profile can be password-protected so that the imported must provide the password in order to import it.

Importing a profile

Only Administrator role users can import profiles.

To import a profile:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Profiles**.
3. Scroll to the bottom of the profiles list and click **Import a Profile**.



Import a Profile

Import a profile, and provide the password that was used to secure it.
Once imported, rename the profile and re-configure it if needed.
Click Save to add this profile to this machine.

Import Profile

Upload location:
Browse... No file selected.

Profile Password

Provide the password used to secure the profile

Profile details

Name

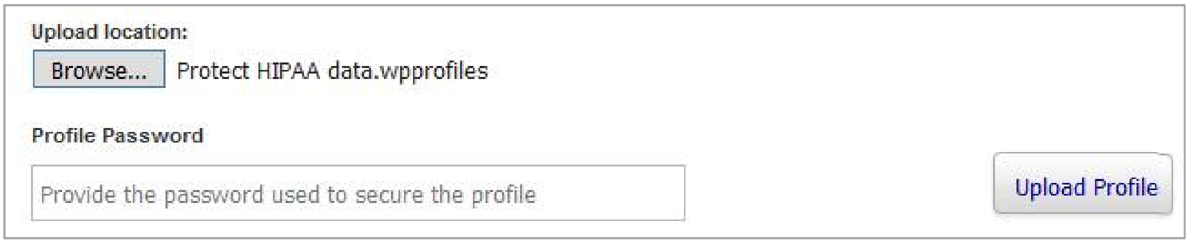
Description

Assign profile to

Email Address
Specify an email address for this profile.
When a user adds this address as a recipient in the email, this profile will be used.

□ Default
□ Fallback

4. Click **Browse** and locate the .wpprofiles file you want to import. Click **Open**.



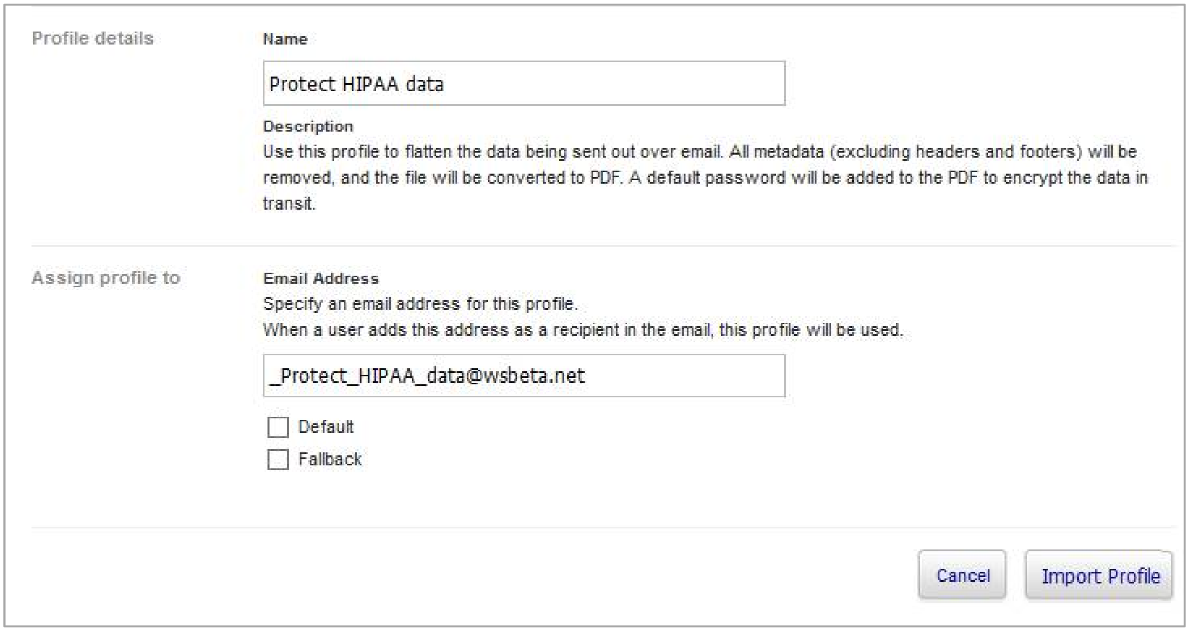
Upload location:
Browse... Protect HIPAA data.wpprofiles

Profile Password

Provide the password used to secure the profile

5. If the profile is password-protected, enter the password.

6. Click **Upload Profile**. Once uploaded, the profile details and email address are populated.



Profile details

Name

Protect HIPAA data

Description

Use this profile to flatten the data being sent out over email. All metadata (excluding headers and footers) will be removed, and the file will be converted to PDF. A default password will be added to the PDF to encrypt the data in transit.

Assign profile to

Email Address

Specify an email address for this profile.

When a user adds this address as a recipient in the email, this profile will be used.

_Protect_HIPAA_data@wsbeta.net

□ Default

□ Fallback

7. Modify the name and email address of the profile if required.

***Note**: The profile description can be modified after the profile has been imported.*

8. Select the **Default** checkbox of you want this profile to be used if no profile email address is specified as a recipient in an email.

9. Select the **Fallback** checkbox if you want this profile to be used when two or more profile email addresses are specified as recipients in an email.

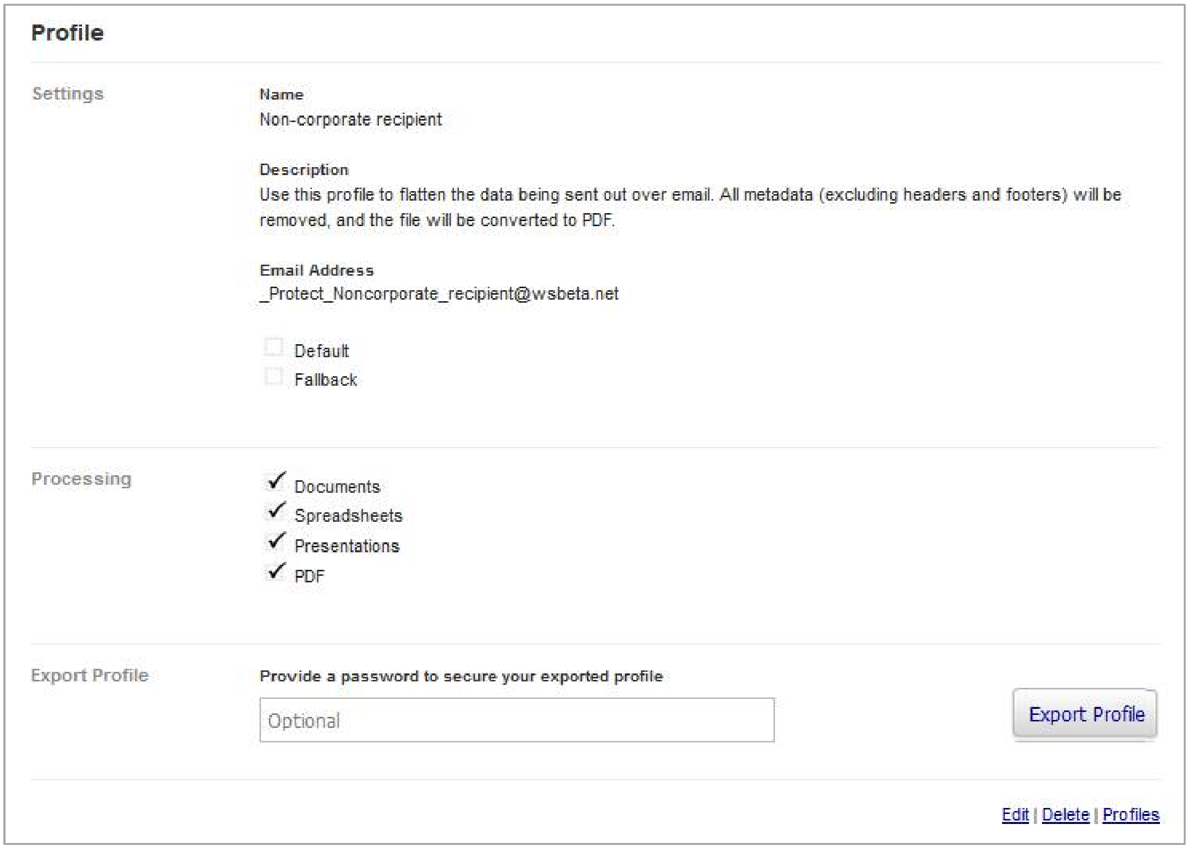
10. Click **Import Profile**. The profile is imported and added to the profiles list

Exporting a profile

Only Administrator role users can export profiles.

To export a profile:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Profiles**.
3. Click the profile name of the profile you want to export.



Profile

Settings

Name
Non-corporate recipient

Description
Use this profile to flatten the data being sent out over email. All metadata (excluding headers and footers) will be removed, and the file will be converted to PDF.

Email Address
_Protect_Noncorporate_recipient@wsbeta.net

□ Default
□ Fallback

Processing

✓ Documents
✓ Spreadsheets
✓ Presentations
✓ PDF

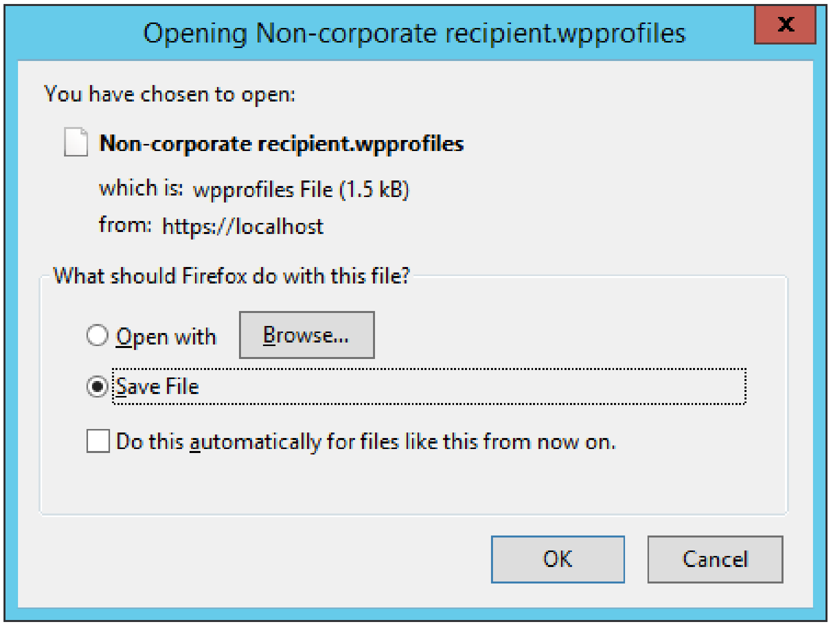
Export Profile

Provide a password to secure your exported profile

Optional

4. If you want to secure the profile so that only administrators who know the password can import it, enter the password in the **Export Profile** area.

5. Click **Export Profile**.



Opening Non-corporate recipient.wpprofiles

You have chosen to open:

Non-corporate recipient.wpprofiles

which is: wpprofiles File (1.5 kB)

from: https://localhost

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

6. Ensure **Save File** is selected and click **OK**. The profile is saved as "[name of profile].wpprofiles" in the default browser downloads location.

Creating Profiles

An Administrator role user can create new profiles.

***Note**: It can take up to a minute for new profiles and changes to existing profiles to take effect.*

When creating profiles, you activate metadata cleaning and select cleaning settings for Microsoft Office (Word, Excel and PowerPoint) and PDF file types individually. You also activate PDF conversion for Microsoft Office file types individually. In this way, you could create a profile, for example, that cleaned metadata from Microsoft Word documents but not from Microsoft Excel or PowerPoint files, or that cleaned comments from Microsoft Word documents and cleaned hidden worksheets, columns and rows from Microsoft Excel spreadsheets, or that converted Microsoft Word and Excel files to PDF but not Microsoft PowerPoint presentations.

Users determine what profile is applied to an email by specifying the profile email address in the **Cc** field.

If a profile email address is specified:

- Workshare Protect Server applies that profile.

If no profile email address is specified:

- Protect Server checks to see what Active Directory group the sender belongs to and then checks to see which profile that Active Directory group has been assigned to. If the Active Directory group is not assigned to any profile, Protect Server will apply the Default profile.
- If the sender belongs to more than one AD group, Protect Server will apply the profile assigned to the more specific group. For example, the sender belongs to “Sales” and also to the sub-group within “Sales” called “Sales UK”. Protect Server will apply the profile assigned to the more specific “Sales UK”. If the sender belongs to two equal groups (at the same depth in the AD hierarchy), for example “Sales UK” and “Sales EMEA”, Protect Server will apply the profile assigned to the highest group in ascending alphabetical order, namely “Sales EMEA”.

If more than one profile email address is specified:

- Protect Server applies the profile that is defined as the Fallback profile.

To create a new profile:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Profiles**.
3. Click **Create**.
4. In the **General** page, complete the general parameters for the profile as follows:

Name The **Name** of the profile appears in notifications indicating which profile was used to process an email.

Description The **Description** of a profile can be used to describe its purpose and provide any additional information of value to administrators.

Email Address The **Email Address** of a profile determines when the profile will be applied. When a user adds this address as a recipient in an email (in the **Cc..** field or the **To..** field) then this profile will be used to process the email.

> ***Warning****: The user should not add the profile email address to the* ***Bcc..*** *field.*

> ***Note****: It is recommended to use an external email domain (may be fictional) for the profile address as it has to be seen as an external address by Microsoft Exchange in order for the preview functionality to work. It is further recommended to add the profile address as an SMTP contact so that it is automatically synchronized between Microsoft Exchange and a user’s global address book.*

Default When **Default** is selected, this profile will be used if no profile email address is specified as a recipient in an email.

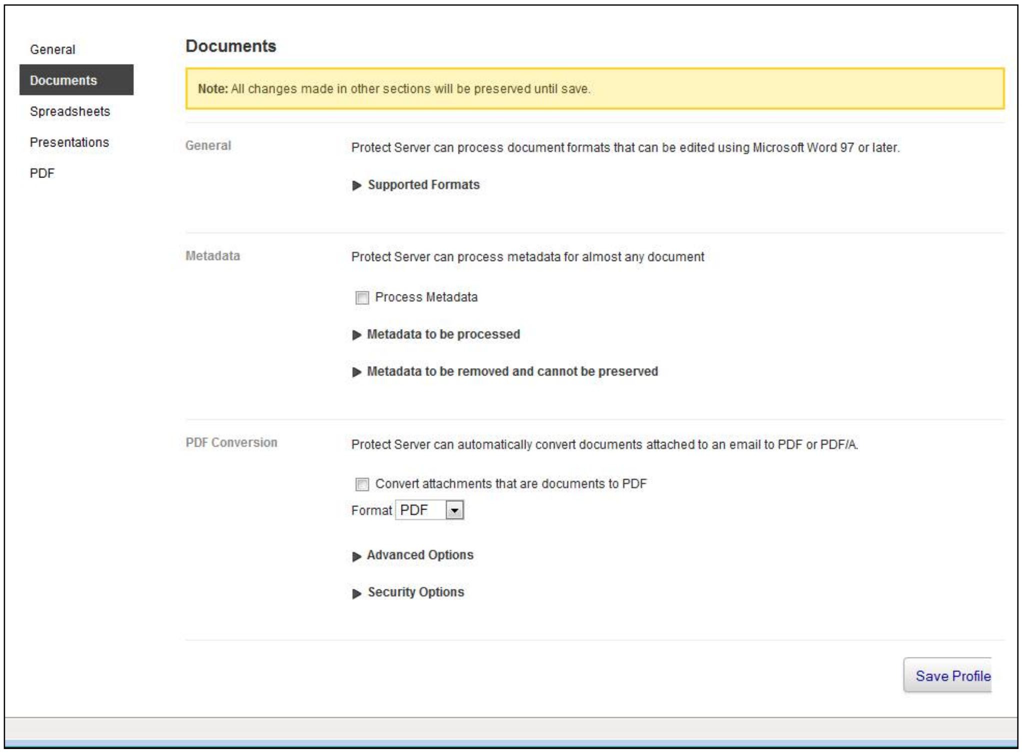
Fallback When **Fallback** is selected, this profile will be used when two or more profile email addresses are specified as recipients in an email.

Active Directory Group Select or specify the Active Directory group to assign to the profile. You may have a tree structure where you can select a group or a text area where you can enter the name of the group. Refer to *Configuring Active Directory Cache Settings* in the *Workshare Protect Server Installation guide*. You can select multiple groups if required. Protect Server will check which AD group the sender belongs to and apply the profile defined for that group.

> ***Note**: If **Configure Active Directory Cache settings** is displayed, you must click this link and configure the AD cache settings in order to be able to select an AD group. Refer to* Configuring Active Directory Cache Settings *in the* Workshare Protect Server Installation guide.

5. Click **Create Profile**. The profile is created. Now you can activate metadata cleaning and select cleaning settings as well as activate PDF conversion for each file type individually.

6. Select **Documents**.



Documents

Note: All changes made in other sections will be preserved until save.

General

Protect Server can process document formats that can be edited using Microsoft Word 97 or later.

▶ **Supported Formats**

Metadata

Protect Server can process metadata for almost any document

□ Process Metadata

▶ **Metadata to be processed**

▶ **Metadata to be removed and cannot be preserved**

PDF Conversion

Protect Server can automatically convert documents attached to an email to PDF or PDF/A.

□ Convert attachments that are documents to PDF

Format PDF

▶ **Advanced Options**

▶ **Security Options**

***Note**: To see the Microsoft Word formats that Protect Server can process and clean, click **Supported Formats**.*

7. Select the **Process Metadata** checkbox to activate metadata cleaning for attachments in Microsoft Word formats.

8. Click **Metadata to be processed**. A list of metadata that can be cleaned from Microsoft Word attachments is displayed.

9. Select which metadata you want to be cleaned from Microsoft Word attachments by selecting the checkbox to the left of the metadata name. Refer to Metadata Cleaned by Workshare Protect Server, for a brief description of each type of metadata.

10. When selecting the following metadata elements, you can click the ⚙ icon to further configure how Protect Server should deal with the metadata:
    - **Bookmarks**: Specify exactly what bookmarks should be removed or preserved.
    - **Built-in Properties**: Specify whether individual properties, such as Author and Category, will be removed, preserved or replaced.
    - **Custom Document Properties**: Specify individual custom properties and whether they will be removed, preserved or replaced.

***Note**: When checking out docx/xlsx/pptx files from Microsoft SharePoint, custom properties **_CheckOutSrcUrl** and **ContentTypeId** are added to the files. Protect Server will remove these if configured to clean custom properties. If you want to preserve these custom properties, you must specify them.*

- **Document Statistics**: Specify whether individual properties, such as Created time and Last Printed time, will be removed, preserved or replaced.
- **Document Variables**: Specify individual document variables and whether they will be removed, preserved or replaced.
- **Embedded Objects**: Specify whether embedded objects, linked objects displayed as icons and linked objects displayed as images should be left alone or converted to images.
- **Fields**: Specify whether individual fields, such as Form Fields and Formulas, will be converted to text or left alone.
- **Redacted Text**: Specify whether to remove or scramble text redacted text of a specific intensity.

***Note**: Removing the redacted text removes it from the document whilst scrambling it, replaces the text with |||||| (thus preserving document layout).*

- **Small Text**: Specify the text size for small text. By default, text smaller than 5 pts is removed.
- **Smart Tags**: Specify how Protect Server will deal with smart tags.

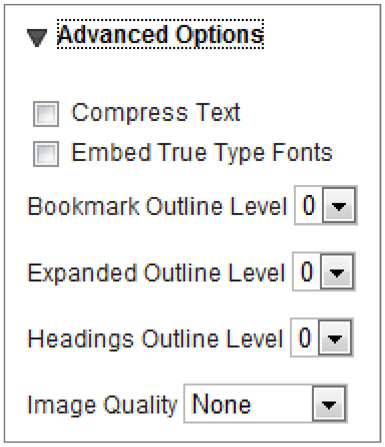
- **White Text**: Specify the intensity for white text.

> ***Note**: Some elements of metadata will always be removed from attachment(s). Click the arrow to the left of **Metadata to be removed and cannot be preserved** to see what metadata is always removed.*

11. Select the **Convert attachments that are documents to PDF** checkbox to activate automatic PDF conversion for attachments in Microsoft Word formats.

12. From the **Format** dropdown list, select whether you want conversion to PDF or PDF/A files.

13. Click **Advanced Options** to display the advanced options for PDF conversion.



▼ Advanced Options

□ Compress Text

□ Embed True Type Fonts

Bookmark Outline Level 0

Expanded Outline Level 0

Headings Outline Level 0

Image Quality None

14. Select from the following settings as required:

Compress Text When **Compress Text** is selected, all text and line art is compressed. This method results in no loss of detail or quality.

Embed True Type Fonts When **Embed True Type Fonts** is selected, a copy of the font used in the attachment is saved inside the PDF file.

Bookmark Outline Level Bookmarks are automatically created in the PDF file based on the bookmarks in the attachment. The **Bookmark Outline Level** specifies the level in the PDF file bookmark outline at which to display the bookmarks. Select from 0 to 9. When **0** is selected, no bookmarks are created; when **1** is selected, bookmarks are created and displayed in the outline at level 1; and so on.

Expanded Outline Level The **Expanded Outline Level** determines how expanded the bookmark outline will be when the PDF file is opened. Select from 0 to 9. When **0** is selected, the bookmarks are completely collapsed; when **3** is selected, the bookmarks are expanded three levels; and so on.

Headings Outline Level Bookmarks are automatically created in the PDF file based on the headings in the attachment. The **Headings Outline Level** specifies the level of heading to use for the bookmarks. Select from 0 to 9. When **0** is selected, no bookmarks are created; when **1** is selected, only heading 1's are converted to bookmarks; and so on.

Image Quality The **Image Quality** determines the clarity of images in the PDF. For example:

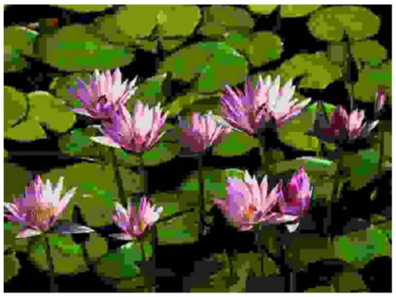
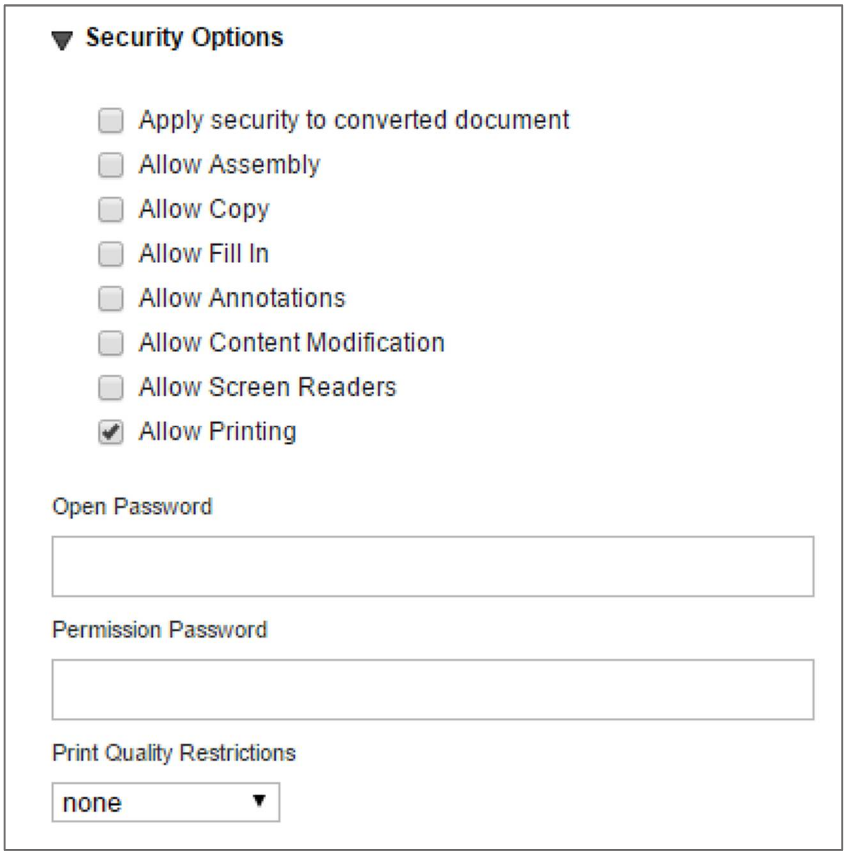


Image Quality = None

Image Quality = Maximum

15. Click **Security Options** to display the security options for PDF conversion.



▼ Security Options

- □ Apply security to converted document
- □ Allow Assembly
- □ Allow Copy
- □ Allow Fill In
- □ Allow Annotations
- □ Allow Content Modification
- □ Allow Screen Readers
- ☑ Allow Printing

Open Password

Permission Password

Print Quality Restrictions

none ▼

16. Select **Apply security to converted document** and select from the following security settings as required:

    Allow Assembly

    When **Allow Assembly** is selected, users can insert, delete, and rotate pages, and create bookmarks and thumbnails in the PDF file.

    Allow Copy

    When **Allow Copy** is selected, users can copy from the PDF file.

    Allow Fill In

    When **Allow Fill In** is selected, users can sign and fill in forms, but not create them in the PDF file.

    Allow Annotations

    When **Allow Annotations** is selected, users can annotate the PDF file using tools from the Commenting toolbar, such as text notes, highlights, lines and circles.

    Allow Content Modifications

    When **Allow Content Modifications** is selected, users can edit the PDF file including modification of text, graphics and pages.

    Allow Screen Readers

    When **Allow Screen Readers** is selected, visually impaired users can read the PDF with screen readers.

    Allow Printing

    When **Allow Printing** is selected, users can print the PDF file.

    Open Password

    When an **Open Password** is specified, users must enter that password before they can open the PDF file.

    Permission Password

    When a **Permission Password** is specified, users must enter that password before they can set or change any security options in the PDF file.

    Print Quality Restrictions

    The **Print Quality Restrictions** determines the availability and quality of printing. The options are as follows:

    - **none**: Prevents users from printing the PDF file.
    - **low resolution**: Users can print at up to 150dpi resolution. Printing can be slower because each page is printed as a bitmap image.
    - **high resolution**: Users can print at any resolution, enabling high quality vector output on Postscript® and other printers that support advanced high quality printing features.

17. Select **Spreadsheets** in the left menu.

18. Repeat steps 7 to 16 to select metadata removal for Microsoft Excel attachments and whether to convert such attachments to PDF.

> ***Note**: For Microsoft Excel attachments, there is no **Format** selection and no **Advanced Options** in the **PDF Conversion** area.*

19. Select **Presentations** in the left menu.
20. Repeat steps 7 to 16 to select metadata removal for Microsoft PowerPoint attachments and whether to convert such attachments to PDF.
21. Select **PDF** in the left menu.
22. Select the **Process Metadata** checkbox to activate metadata cleaning for PDF attachments.
23. Click **Metadata to be processed**. A list of metadata that can be cleaned from PDF attachments is displayed
24. Select which metadata you want to be cleaned from PDF attachments by selecting the checkbox to the left of the metadata name. Refer to Metadata Cleaned by Workshare Protect Server, for a brief description of each type of metadata.
25. Click **Security Options** to display the security options for the PDF attachment.
26. Select **Apply security to converted document** and select from the security settings as required. Refer to step 16 for a description of the security settings.
27. When you have made the required selections, click **Save Profile**. The settings are saved into the profile and the profile is displayed in the list of profiles on the Profiles page.

Chapter 3: Reviewing Message Logs

This chapter describes the message logs provided by Workshare Protect Server. It includes the following sections:

- **Introducing Workshare Protect Server Message Logs**, page 28, introduces the message logs produced by Protect Server.
- **Viewing Emails**, page 28, describes how to search through the emails processed by Protect Server.

This functionality is available for all role users. However, the functionality differs, as follows:

- *Administrator role users can search through all emails processed by Protect Server.*
- *Business and User role users can only search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.*

Introducing Message Logs

Message logs provide information about all the emails processed by Workshare Protect Server. The message logs can be searched and accessed through the **Messages** tab of the Protect Server web console.

Viewing Emails

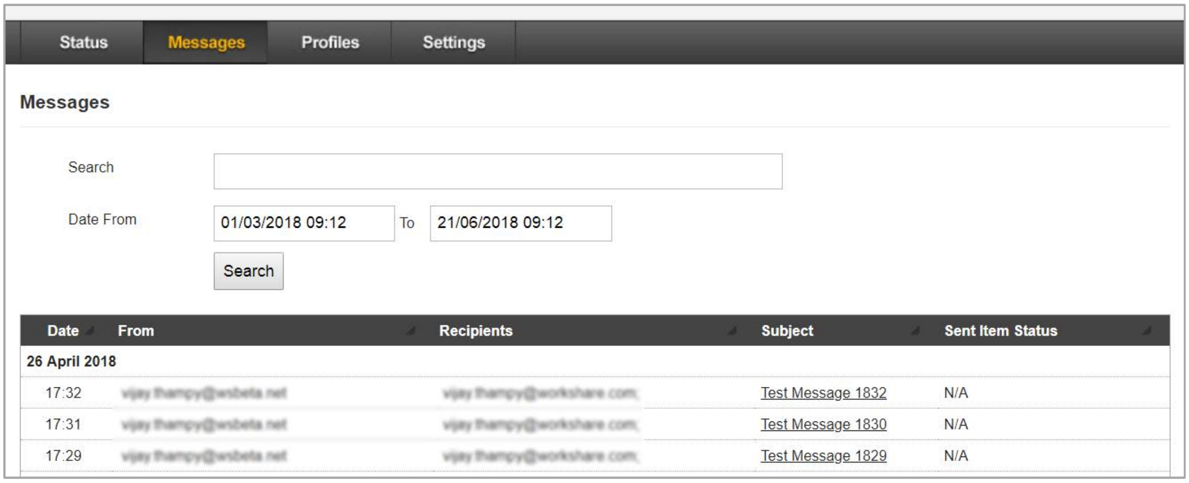
The **Messages** tab is available to all role users. However, Administrator role users can search through all emails processed by Workshare Protect Server whereas Business and User role users can only search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.

To search message logs:

1. Log into the Protect Server web console.
2. Select **Messages**.
3. In the **Search** field, enter your search criteria. Protect Server searches for the keyword(s) in the senders/recipients names, subject, attachment names and metadata item name.

> ***Note**: Use double quotes (“) around attachment names and sender/recipients in order for the search not to break up the terms between periods (.) or the @ sign.*

4. Enter a date range if required.
5. Click **Search**. The emails that have passed through Protect Server and match your search criteria are displayed.



Messages

Search

Date From 01/03/2018 09:12 To 21/06/2018 09:12

Date	From	Recipients	Subject	Sent Item Status
26 April 2018				
17:32	[redacted]	[redacted]	Test Message 1832	N/A
17:31	[redacted]	[redacted]	Test Message 1830	N/A
17:29	[redacted]	[redacted]	Test Message 1829	N/A

Tip! *To display all emails that have passed through Protect Server, leave the* ***Search*** *field blank and click* ***Search****.*

For each email, the following information is provided:

Date The date the email was sent.

From The email address of the sender of the email.

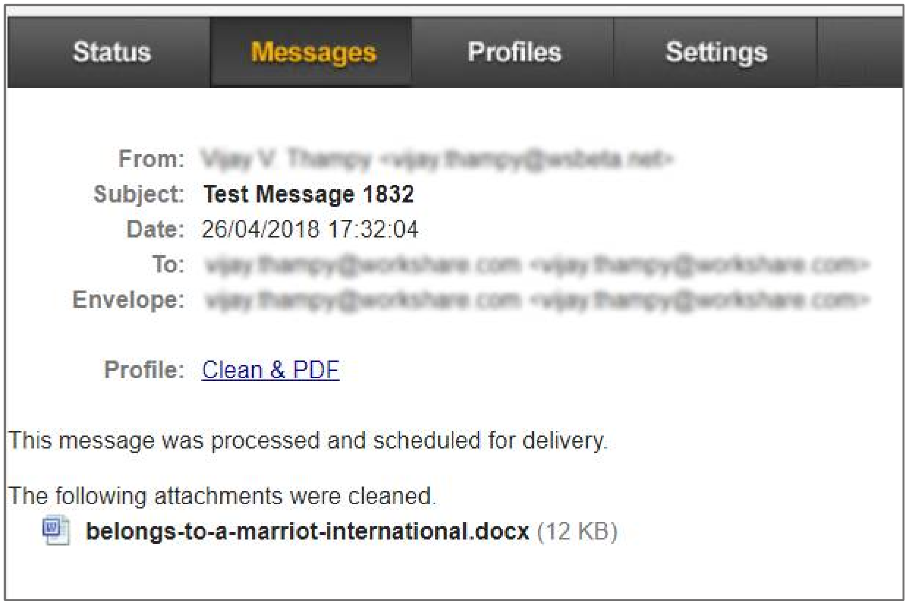
Recipients The email address(es) of the recipient(s) of the email.

Subject The subject matter of the email, as entered in the **Subject** field.

Sent Item Status The synchronization status. The status can be:

- **Updated**: Email in Sent items updated with processed email.
- **Pending**: Waiting to update email in Sent items with processed email.
- **Error**: Pending Retry: Error when trying to update email in Sent items with processed email, waiting to retry update.
- **Failed (receipt sent)**: Failed to update email in Sent items with processed email, clean receipt sent to sender.
- **Failed (email copied)**: Failed to update email in Sent items with processed email, a copy of the processed email added to Sent items folder.
- **Failed**: Failed to update email in Sent items with processed email.
- **N/A**: Synchronization not enabled.

Click the **Subject** of an email to display further details. For example:



From: [redacted]
Subject: **Test Message 1832**
Date: 26/04/2018 17:32:04
To: [redacted]
Envelope: [redacted]

Profile: Clean & PDF

This message was processed and scheduled for delivery.

The following attachments were cleaned.

belongs-to-a-marriot-international.docx (12 KB)

You can now see which profile was applied to the email attachment and if you have configured Protect Server to store a copy of the cleaned message in the database, you can also download the processed attachment if required. Click the profile link to view the properties of the profile in the **Profiles** tab of the Protect Server web console.

Appendix A. Metadata that can be Cleaned

This appendix provides a brief description of the different types of metadata that Workshare Protect Server can clean from attachment(s).

Metadata Cleaned by Workshare Protect Server

Annotations and markup

Select this option to remove markup from a PDF file.

Description	Risk	Applies to
Markup is a tool used to make comments and annotations to PDF documents.	The annotations may contain sensitive data.	PDF.

Attached template

Select this item to reset the document template to the default template. 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.

Description	Risk	Applies to
Microsoft Word ships with templates for many common business documents. NORMAL.DOT is the default template for Word 97 through Word 2003 and NORMAL.DOTX is the default template for Word 2007.	The attached template contains the fully qualified path of the template that was used to create the document. It may contain a server name or user name that you do not want to expose to outside parties.	All versions of Microsoft Office (97 and above).

Attachments

Select this option to remove attachments from a PDF file.

Description	Risk	Applies to
PDF attachments are separate files contained within the PDF document.	Metadata and sensitive data may be included in files attached within the PDF.	PDF.

Bookmarks

Select this option to remove bookmarks or text contained within bookmarks from a document.

Description	Risk	Applies to
Bookmarks are used to aid document navigation and automation. Users can create bookmarks that link to a particular section of text or act as placeholders for data populated during document automation, which involve third-party macros. Bookmarks may also be placeholders for paragraphs, which can be freely edited during production.	The names of hidden bookmarks can reveal the context of information contained within the document. Bookmarks are also a consequence of form fields, so even after form fields are removed, it is still possible to identify the data of the form fields through the bookmarks that are left behind when they are unlinked.	All versions of Microsoft Word (97 and above) and PDF.

Built-in properties

Select this option to remove built-in properties from a document.

Description	Risk	Applies to
Built-in properties are details about a file that help identify it, including its title, subject, author, manager, company, category, keywords, comments, and hyperlink base.	The names of authors and the name of the company can display sensitive information about your corporation or customers. It is possible that if a document has been sent outside your firewall, the author name and company name contained in the built-in properties could be a name other than your own. In addition, if documents are re-purposed or used as a template for a new document, information that is specific to a previous client or the client's name can be stored as hidden information within the new document.	All versions of Microsoft Office (97 and above).

Comments

Select this item to remove comments from a document.

Description	Risk	Applies to
Comments are notes and suggestions that are added to a document via the comment feature to aid collaborative online review.	Comments can display sensitive information about your corporation or customers and can result in embarrassing situations where external parties are able to view proprietary information.	All versions of Microsoft Office (97 and above).

Content controls

Select this item to remove all content controls from a document.

Description	Risk	Applies to
Content controls are used in structured documents to control how the layout, behavior, and properties (for example) of pre-defined document elements. Content controls can be used, for example, to make boilerplate text in a pre-defined disclaimer element unalterable by users.	Like custom XML, content controls can reveal sensitive information about a document, your corporation or its customers including links to network servers and database records. Content controls may describe the snippets of text contained therein and may provide context to a reader (for example, a document version number).	Microsoft Word 2007 (DOCX files).

Custom document properties

Select this option to remove custom properties from a document.

Description	Risk	Applies to
Custom properties are those you define. You can assign a text, time, or numeric value to custom properties, or assign them the values "yes" or "no." You can also choose from a list of suggested names or define your own. You can optionally link custom document properties to specific items in your file, or a bookmark. For example in a contract form created in Word, you can create a custom file property that is linked to a form field that contains the contract's expiry date. Then you can search for all contract files with expiry dates earlier than a date you specify.	Custom Properties are generally specific to an organization; they may include a document number, matter or case number, personal information, or variables used in payment calculations, for example, rate per hour. They may also contain information that links the document to a DMS, CRM, or matter management system.	All versions of Microsoft Office (97 and above)

Custom XML

Protect Server removes all custom XML from a document.

Note: *You cannot configure this option.*

Description	Risk	Applies to
XML support lets you add structured-data elements to documents, thereby expediting automation and enabling interaction with other business applications that use structured data.	Custom XML can reveal sensitive information about a document, your corporation or its customers.	Microsoft Word 2007 (DOC and DOCX files).

Document properties

Select this option to remove standard properties from a PDF file.

Description	Risk	Applies to
Standard properties are details about a file that help identify it, including its title, subject, author, manager, company, category, keywords, comments, and hyperlink base.	The names of authors and the name of the company can display sensitive information about your corporation or customers. It is possible that if a PDF has been sent outside your firewall, the author name and company name contained in the standard properties could be a name other than your own. In addition, if files are re-purposed or used as a template for a new file, information that is specific to a previous client or the client's name can be stored as hidden information within the new file.	PDF.

Document statistics

Select this option to remove document statistics from a document.

Description	Risk	Applies to
Document statistics include information on when the document was created, when it was modified, when it was accessed, and when it was printed. In addition, document statistics display the name of the person it was last saved by, the revision number, and the total editing time. Other statistics include number of pagers, paragraphs, lines, words, and characters.	Document statistics can create embarrassing situations when the hours billed do not match the total editing time. In addition, the "last saved by" metadata shows the last person who edited the document. This can be risky if it is discovered that the person whose rate and time is billed out is different from the person who actually worked on the document.	All versions of Microsoft Office (97 and above).

Document variables

Select this option to remove document variables from a document.

Description	Risk	Applies to
Document variables are values stored in Microsoft Word documents that are used by either field codes or macros.	These variables may contain confidential information such as company names, client-specific information or information that links the document to a DMS or CRM system. Even if field codes and macros are removed, the variables used may remain in the document.	All versions of Microsoft Word (97 and above).

Embedded objects

Select this option to convert embedded or linked objects (such as spreadsheets contained within or linked to a Word document) to images.

Description	Risk	Applies to
These objects may appear either as another document nested within the body of a Word document, or as a connection to another document. An embedded object is information contained in a source file and inserted into a destination file. Once embedded, the object becomes part of the destination file and any changes you make to the embedded object are reflected in the destination file. A linked object is an object that is created in a source file and inserted into a destination file, while maintaining a connection between the two files. The linked object in the destination file can be updated when the source file is updated.	Embedded objects can include proprietary information about your corporation or its customers. ***Note****: When you activate an embedded object in a document, only part of the embedded object is displayed within the document; the object may contain additional information that does not appear. If you want a document to contain only a rendering of the embedded object and not the actual contents, cut the object and then use* ***Paste Special*** *on the Edit menu to paste the object into the document using a Metafile format. After you do this, you can no longer edit the embedded object; however, it will not contain any metadata.*	All versions of Microsoft Word and Excel (97 and above).

Endnotes

Select this option to remove endnotes from a document.

Description	Risk	Applies to
Endnotes are text inserted at the end of a document.	While not typically considered metadata, endnotes may contain sensitive information such as instructions to users for completing a form.	All versions of Microsoft Word (97 and above).

External links

Select this item to convert external links in cells in an Excel spreadsheet to text.

Description	Risk	Applies to
External links are links from cells to another file. For example: Link to a cell in another Microsoft Excel worksheet; named link to a named reference in another worksheet; link to another worksheet; OLE link that inserts another document as an icon; or OLE link that inserts another document as text.	Links can maintain a link to a file that corporations may not wish to disclose such as files on a computer's local file system, on a corporation's internal file share, or on an intranet.	All versions of Microsoft Excel.

Fast saves

Protect Server removes previous iterations of the document created via a fast save.

***Note:** You cannot configure this option.*

Description	Risk	Applies to
Fast saves is an option in Microsoft Word 2003 (SP2 and earlier) that saves only the changes made to a document at the end of the document. The deleted content is not overwritten in the document and can be viewed when saving the document as “recovered text.” Disabling fast saves and saving the document will perform a full save, overwriting previously removed content from the document so that the deleted content can no longer be read as “recovered text.”	Like other metadata, changes saved during a fast save can expose sensitive information to external parties when viewed using a text or hex-editor. Deleted text can still exist in the electronic file.	Microsoft Word 97 through to 2003 SP2 (DOC files only).

Fields

Select this option to convert fields in a document to text.

Description	Risk	Applies to
Word uses field codes as placeholders for dynamic data which it updates automatically when you perform routine tasks. For example, when you insert a page number, when you insert a document building block such as a cover page, or when you create a table of contents. You can also manually insert fields to automate aspects of your document, such as merging data from a data source or performing calculations. In Microsoft Office Word 2007, there is little need to insert fields manually, because built-in commands and content controls provide most of the capabilities that fields provided for many versions of Word.	Left unaltered, field codes that reference built-in or custom properties may be exposed. Field codes can be visible to anyone reading your document, a risk if the information you place in field codes is information that you want kept private.	All versions of Microsoft Word (97 and above) and PDF.

Fields (PDF)

Select this option under **Metadata to be processed** to remove fields from a PDF file or select this option under **Metadata to be flattened** to convert fields to text.

Description	Risk	Applies to
Fields in a PDF can make it into an interactive form.	Left unaltered, field codes that reference built-in or custom properties may be exposed.	PDF.

Footers

Select this item to remove footers from a document.

Description	Risk	Applies to
Footers are areas at the bottom of some or all pages in a document. Footers can contain text deemed to be metadata, such as the author, document number, case or matter information, whether it's confidential, a draft document or not. Footers can also contain information that may not be considered metadata, such as page numbers, document title and so on.	Custom footers can contain descriptions such as filename, path, the date and time the document was modified or other information used to track a file. Unfortunately, users often overlook footers when preparing a document for distribution. Failure to remove this information can expose confidential information.	All versions of Microsoft Word and Excel (97 and above).

Footnotes

Select this item to remove footnotes from a document.

Description	Risk	Applies to
Footnotes are commonly used to annotate text in the body of a document. They appear on the same page as the referenced text.	While not typically considered metadata, footnotes may contain instructions about how to complete parts of the document.	All versions of Microsoft Word (97 and above).

Formulas

Select this item to convert formulas in a document to text.

Description	Risk	Applies to
Formulas are equations used to calculate values.	Left unaltered, formula codes that reference sensitive information or other workbooks may be exposed.	All versions of Microsoft Excel (97 and above).

Headers

Select this item to remove headers from a document.

Description	Risk	Applies to
Headers are areas at the top of some or all pages in a document. Headers can contain text deemed to be metadata, such as the author, document number, case or matter information, whether it's confidential, a draft document or not. Headers can also contain information that may not be considered metadata, such as page numbers, document title and so on.	Custom headers can contain descriptions such as filename, path, the date and time the document was modified or other information used to track a file. Unfortunately, users often overlook headers when preparing a document for distribution. Failure to remove this information can expose confidential information.	All versions of Microsoft Word and Excel (97 and above).

Hidden columns

Select this item to remove hidden columns from a spreadsheet.

Description	Risk	Applies to
Hidden columns are columns that have been formatted as hidden.	Hidden columns can contain confidential information and can potentially be viewed by third parties.	All versions of Microsoft Excel (97 and above).

Hidden rows

Select this item to remove hidden rows from a spreadsheet.

Description	Risk	Applies to
Hidden rows are rows that have been formatted as hidden.	Hidden rows can contain confidential information and can potentially be viewed by third parties.	All versions of Microsoft Excel (97 and above).

Hidden slides

Select this item to remove hidden slides from a presentation.

Description	Risk	Applies to
Hidden slides are slides that have been formatted as hidden.	Hidden slides can contain confidential information and can potentially be viewed by third parties.	All versions of Microsoft PowerPoint (97 and above).

Hidden text

Select this item to remove hidden text from a document.

Description	Risk	Applies to
Hidden text is text that has been formatted as hidden. Unless specifically selected to be viewed in Microsoft Word, hidden text is not displayed within the document. Depending on the settings in Word, hidden text may be printed.	Hidden text can contain notes and instructions that are particular to a document. As hidden information that is not cleaned, the hidden text can potentially be viewed by third parties.	All versions of Microsoft Word (97 and above).

Hidden worksheets

Select this item to remove hidden worksheets from a spreadsheet.

Description	Risk	Applies to
Hidden worksheets are worksheets that have been formatted as hidden.	Hidden worksheets can contain confidential information and can potentially be viewed by third parties.	All versions of Microsoft Excel (97 and above).

Highlighted text

Select this item to remove highlighted text from a document.

Description	Risk	Applies to
Users use highlighting in the same way they use comments or to draw attention to some text in the body of a document. This is especially useful in collaborative efforts; one user might highlight a passage of text indicating to others that he or she needs more input, for example.	Highlighted text may contain notes and sensitive information.	All versions of Microsoft Word (97 and above).

Hyperlinks

Select this item to remove hyperlinks from a document. The linked text is preserved but the associated hyperlinks are removed.

Description	Risk	Applies to
Hyperlinks can be used to link to confidential documents, email addresses, file shares, or intranet addresses.	Hyperlinks can maintain a link to a site that corporations may not wish to disclose such as files on a computer's local file system, on a corporation's internal file share, or on an intranet.	All versions of Microsoft Word and Excel (97 and above).

***Note:** Custom hyperlinks are distinct from system-generated hyperlinks used to build and maintain a document's table of contents, index, and table of authorities.*

Macros

Select this item to remove Visual Basic macros from the document. This feature is not intended as virus protection, but rather to protect any confidential information, intellectual property, or formulas included in the macros.

Description	Risk	Applies to
Word users can automate repeated tasks using macros. A macro is a series of commands and instructions that are grouped together as a single command to accomplish a task automatically.	Macros can be set for templates that may have some amount of pre-populated data. There may be a time when the information contained in these templates should not be seen by external audiences. In another situation, macros may contain information about internal databases, file shares, document management or CRM systems, or information stored on an intranet. Lastly, macros are often quite complex and, if developed in-house, may represent the company's intellectual property. If macros are included in the document, the information is freely shared with outside parties.	All versions of Microsoft Office (97 and above) DOC and DOCM files only - not supported in RTF or XML files.

Presentation tags

Select this option to remove presentation tags from a presentation.

Description	Risk	Applies to
Presentation tags are a feature of Microsoft PowerPoint (accessed using VBA) that allows custom information to be associated with objects in the presentation.	The tags may contain sensitive data.	Microsoft PowerPoint (97 and above).

Previous authors

Protect Server removes information about previous authors from a document.

***Note:** You cannot configure this option.*

Description	Risk	Applies to
Previous author information is information about all authors who have previously saved the document as well as save locations.	The names of authors can display sensitive information about your corporation or customers.	All versions of Microsoft Word (97 and above).

Redacted text

Select this option to remove or scramble redacted text. Removing the redacted text removes it from the document whilst scrambling it, replaces the text with |||||| (thus preserving spreadsheet layout). Redacted text is any non-white text that has a matching background thus making the text illegible, for example, black on black.

Description	Risk	Applies to
Redacted text is where the font and background color are the same or nearly the same. When the font and background color match exactly, the text is invisible when the document is viewed or printed. Backgrounds include highlighting; as well as text, cell, and textbox shading.	Depending on its content, redacted text can be very damaging. Redacted text may contain private information about clients' as well proprietary information about your corporation.	All versions of Microsoft Word and Excel (97 and above).

Routing slip

Protect Server removes the routing slip from a document.

***Note:** You cannot configure this option.*

Description	Risk	Applies to
Routing slips are used to create a distribution list of reviewers in a particular order. Routing slips are manually created by adding in recipients' email addresses. When a file is routed, its routing slip is sent as an email attachment.	Routing slips reveal the names of the people that the document was sent to for review. This may be information that should stay confidential rather than distributed externally. An example of how this information can be used is when email addresses are put in the routing slips. If this document is then published to the Internet, the email address can be displayed for all to see. This also deletes any envelope information, such as recipients, subject, and introduction, which are used when sending to a mail recipient.	Microsoft Word and Excel 97 through to 2003 SP2 (DOC/XLS files only).

Slide tags

Select this option to remove slide tags from a presentation.

Description	Risk	Applies to
Slide tags are a feature of Microsoft PowerPoint (accessed using VBA) that allows custom information to be associated with objects in the presentation.	The tags may contain sensitive data.	Microsoft PowerPoint (97 and above).

Small text

Select this option to remove small text from a document.

Description	Risk	Applies to
Any text block contained in a document that is smaller than 5 points (i.e. 4pts and less) is considered small text. The text is so small that it will not be visible when viewed or printed and can be used to hide information in a document.	Small text is often used for instructions users must follow when completing the document. Such instructions may be proprietary and contain sensitive information.	All versions of Microsoft Office (97 and above).

Smart tags

Select this option to remove smart tags from a document.

Description	Risk	Applies to
Smart tags are used to identify and provide context for particular text in a document (such as a person's name), and to allow users to perform certain actions when they select the text.	Depending on the smart tag functions you use, they may embed extra hidden information in your document such as a confidential telephone number or contact.	Microsoft Word XP and above.

Speaker notes

Select this item to remove speaker notes from a presentation.

Description	Risk	Applies to
Speaker notes are notes added to presentation slides as a reference for the presenter. They are an area of a presentation or slide that is hidden during the presentation and is reserved for notes for the speaker.	Speaker notes can include important key points to cover during a presentation. This information may be confidential or sensitive information about your corporation or customers.	All versions of Microsoft PowerPoint (97 and above).

Track changes

Select this item to accept all changes made to a document and turn off change tracking in the processed document.

Description	Risk	Applies to
As with comments, users often enable change tracking to capture successive edits made to a collaborative document.	Changes that are not accepted still remain with the document, even though they appear to be invisible. These changes can easily be displayed by turning on the "Show markup view." This can result in embarrassing situations where external parties are able to view proprietary information.	All versions of Microsoft Word and Excel (97 and above).

Track change authors

Select this item to leave track changes in a document but remove the change author information in the processed document.

Description	Risk	Applies to
The track change author is the user who makes changes to a document.	The names of authors can display sensitive information about your corporation or customers.	All versions of Microsoft Word (97 and above).

Track change timestamps

Select this item to leave track changes in a document but remove the timestamp of the tracked change in the processed document.

Description	Risk	Applies to
The track change timestamp is the time the change was made to a document.	The timestamps can display sensitive information about your corporation.	All versions of Microsoft Word (97 and above).

Unused masters

Select this item to remove unused masters from a presentation.

Description	Risk	Applies to
Unused masters are unused master slides.	The unused masters may contain sensitive data.	All versions of Microsoft PowerPoint (97 and above).

Versions

Protect Server removes the version number from a document and turns off auto-versioning.

***Note:** You cannot configure this option.*

Description	Risk	Applies to
Some versions of Microsoft Word record the number of times a document has been versioned over its lifetime. This function enables Microsoft Word to save prior versions of a document as a part of the electronic file.	If unaltered, a document's recipient can access any of the previous versions that have been saved and see how the document was changed over time. This metadata, while useful in some instances, can disclose sensitive information.	Microsoft Word 97 to 2003 (DOC files only).

Watermarks

Select this item to remove a watermark from a document.

Description	Risk	Applies to
Watermarks are often used internally to designate the state of a document, such as "Draft".	Because watermarks are configurable, they can contain sensitive information about your corporation or its customers.	All versions of Microsoft Word (97 and above).

White text

Select this item to remove white text (white text on a white background) from a document.

Description	Risk	Applies to
White text is text formatted as white on a background that is formatted as white. White text is text has been formatted with a font color of white and has no background color.	Depending on its content, white text can be very damaging. White text may contain private information about clients' as well proprietary information about your corporation.	All versions of Microsoft Word and Excel (97 and above).

Worksheet properties

Select this option to remove worksheet properties from a spreadsheet.

Description	Risk	Applies to
Worksheet properties are details about a spreadsheet that help identify it. They are added using VBA.	Properties can display sensitive information about your corporation or customers. In addition, if spreadsheets are re-purposed or used as a template for a new spreadsheet, information that is specific to a previous client can be stored as hidden information within the new spreadsheet.	All versions of Microsoft Excel (97 and above).

XML comments

Protect Server removes XML comments from a file.

***Note:** You cannot configure this option.*

Description	Risk	Applies to
XML comments are similar to HTML comments. The comments are added as notes or lines for understanding the purpose of XML code. Comments can be used to include related links, information, and terms. They are visible only in the source code; not in the XML code. Comments may appear anywhere in XML code.	Comments can display sensitive information about your corporation or customers and can result in embarrassing situations where external parties are able to view proprietary information.	Microsoft Office (DOCX, XLSX, PPTX) files.

Appendix B. Metadata Cleaning

This appendix provides information on the metadata that can be cleaned by Workshare Protect Server as well as by Workshare Protect Desktop.

Metadata Cleaning by Workshare Protect Server

The following table indicates what types of metadata Workshare Protect Server can clean from different file formats. The following symbols are used:

✓	Metadata that can be cleaned
✔	Metadata that is not preserved, meaning it is always removed
✗	Metadata that cannot be cleaned
empty	Metadata is not found in this file format

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Attachments									✓
Bookmarks	✓	✓	✓	✓					✓
Built-in properties	✓	✓	✓	✓	✓	✓	✓	✓	
Comments	✓	✓	✓	✓	✓	✓	✓	✓	
Content controls		✓		✓					
Custom properties	✓	✓	✓	✓	✓	✓	✓	✓	
Custom XML		✔							
Document properties									✓
Document statistics	✓	✓	✓	✓	✓	✓	✓	✓	
Document variables	✓	✓	✓	✓					
Embedded objects	✓	✓	✓	✓	✓	✓	✗	✗	
Endnotes	✓	✓	✓	✓					
External links					✓	✓			
Fast saves	✔								

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Fields	✗	✗	✓	✓					✓
Footers	✓	✓	✓	✓	✓	✓	✗	✗	✗
Footnotes	✓	✓	✓	✓					✗
Formulas					✓	✓			
Headers	✓	✓	✓	✓	✓	✓	✗	✗	✗
Hidden columns					✓	✓			
Hidden rows					✓	✓			
Hidden slides							✓	✓	
Hidden text	✓	✓	✓	✓					
Hidden worksheets					✓	✓			
Highlighted text	✓	✓	✓	✓					✗
Hyperlinks	✓	✓	✓	✓	✓	✓	✗	✗	✗
Ink annotations	✗	✗	✗	✗	✗	✗	✗	✗	
Macros	✓	✓ docm		✓	✓	✓ xlsm	✓	✓ pptm	
Markup									✓
Presentation tags							✓	✓	
Previous authors	✓								
Redacted text	✓	✓	✓	✓	✓	✓	✗	✗	✗
Routing slip	✓				✓		✗		
Slide tags							✓	✓	
Small text	✓	✓	✓	✓	✓	✓	✓	✓	✗
Smart tags	✓	✓	✓	✓					
Speaker notes							✓	✓	

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Attached templates	✓	✓	✓	✓	✓	✓	✓	✓	
Track changes	✓	✓	✓	✓	✓	✓			
Track change authors	✓	✓	✓	✗	✗	✗			
Track change timestamps	✓	✓	✓	✗	✗	✗			
Unused masters							✓	✓	
Versions	✓								
Watermarks	✓	✓	✓	✓					✗
White text	✓	✓	✓	✓	✓	✓	✗	✗	✗
Worksheet properties					✓	✓			
XML comments	✓	✓		✓	✓	✓	✓	✓	

Metadata Cleaning by Workshare Protect Client

The following table indicates what types of metadata the Workshare Protect Desktop cleans from different file formats. The following symbols are used:

✓	Metadata that can be cleaned
✗	Metadata that cannot be cleaned
empty	Metadata is not found in this file format

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Attachments									✓
Bookmarks	✗	✗	✗	✗	✗	✗	✗	✗	✓
Built-in properties	✓	✓	✓	✗	✓	✓	✓	✓	

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Comments	✓	✓	✓	✗	✓	✓	✓	✓	
Content controls		✗		✗					
Custom properties	✓	✓	✓	✗	✓	✓	✓	✓	
Custom XML		✗							
Document properties									✓
Document statistics	✓	✓	✓	✗	✗	✗	✗	✗	
Document variables	✓	✓	✓	✗					
Embedded objects	✓	✓	✓	✗	✓	✓	✗	✗	
Endnotes	✗	✗	✗	✗					
Fast saves	✓								
Fields	✓	✓	✓	✗					
Footers	✗	✗	✗	✗	✓	✓	✓	✓	✗
Footnotes	✓	✓	✓	✗					✗
Formulas					✗	✗			
Headers	✗	✗	✗	✗	✓	✓	✓	✓	✗
Hidden columns					✗	✗			
Hidden rows					✗	✗			
Hidden slides							✓	✓	
Hidden text	✓	✓							
Hidden worksheets					✗	✗			
Highlighted text	✓	✓	✓	✗					
Hyperlinks	✓	✓	✓	✗	✓	✓	✓	✓	✗
Ink annotations	✓	✓	✓	✗	✓	✓	✓	✓	

Hidden data	doc	docx	rtf	xml 2007	xls	xlsx	ppt	pptx	pdf
Macros	✓	✓ docm			✓	✓ xlsm	✓	✓ pptm	
Markup									✓
Presentation tags							✗	✗	
Previous authors	✓	✓							
Redacted text	✓	✓	✓	✗	✗	✗	✗	✗	✗
Routing slip	✓				✗		✗		
Slide tags							✗	✗	
Small text	✓	✓	✓	✗	✗	✗	✗	✗	✗
Smart tags	✓	✓	✓	✗					
Speaker notes							✓	✓	
Attached templates	✓	✓	✓	✗	✗	✗			
Track changes	✓	✓	✓	✗	✓	✓			
Unused masters							✗	✗	
Versions	✓								
Watermarks	✗	✗	✗	✗					✗
White text	✓	✓	✓	✗	✗	✗	✗	✗	✗
Worksheet properties					✗	✗			
XML comments	✗	✗		✗	✗	✗	✗	✗	

Copyright

Disclaimer

The authors/publishers of this guide and any 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 this 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.

Revisions

Published for Workshare Protect Server 3.10: 29/06/18
Published for Workshare Protect Server 3.11: 24/08/18

Sold under a license for U.S. Patent Nos. 7,895,276 and 8,060,575 and 8,977,697.

Workshare Ltd., 20 Fashion Street, London E1 6PX www.workshare.com