

Workshare Policy Designer User Guide

Table of Contents

Chapter 1: Introducing Workshare Policies	5
What are Policies?	6
Key points	6
Key terms	6
What is monitored?	7
Default policies	7
What Policy does Protect Apply?	9
How to configure Protect	10
Creating Policies in the Policy Designer	13
Chapter 2: Installing the Policy Designer	15
Installation Overview	16
Upgrading from Earlier Versions	16
Running the Install	17
Chapter 3: Quick Tour of the Policy Designer	20
Accessing the Workshare Policy Designer	21
Workshare Policy Designer Main Window	22
Toolbar icons	22
File menu	22
Edit menu	23
Tools menu	23
Windows menu	24
Help menu	24
Language settings	24
Chapter 4: Policy Sets and Policies	25
Creating Policy Sets	26
Terms and concepts	26
Building a policy	26
Creating a new policy set	27

Opening the default and existing policy sets	29
Creating New Policies	30
Viewing and Editing Existing Policies	31
Copying Policies	32
Deleting Policies	32
Chapter 5: Conditions and Expressions	33
Defining Conditions	34
Viewing and editing existing expressions	37
Deleting expressions	37
What users see	38
Configuring Expressions	39
Rules about expressions	39
<u>file type</u> contains <u>word or phrase</u> within <u>context</u> of the file	39
<u>file type</u> contains <u>regular expression</u> within <u>context</u> of the file	41
<u>file type</u> contains <u>PII type</u>	43
<u>file type</u> contains <u>hidden data</u>	45
PDF file contains <u>hidden data</u>	47
<u>file type</u> is password protected	48
custom property <u>name</u> is <u>value</u>	48
file size is <u>compared against size</u> Kb	49
file type is <u>file type</u>	50
contains embedded email	50
Email has <u>email address or domain</u> within <u>recipients</u> address fields	51
Email has only <u>email address or domain</u> within <u>recipients</u> address fields	52
Total attachment size is <u>compared against size</u> Kb	53
Chapter 6: Channels and Action Sets	54
Introducing Channels and Action Sets	55
Client Email Channel	55
Routing for Client Email channel	56
Creating action sets for Client Email channel	63

Active Content Channel	72
Chapter 7: Policy Activation	75
Publishing Policy Sets	76
Chapter 8: Language Files	78
Overview of Language Files	79
Exporting a Language File from a Policy Set	79
Importing a Language File into a Policy Set	80
Appendix A.Regular Expressions	81
Introducing Regular Expressions	82
Regular Expression Applications	82
Useful references	82
Appendix B.Clean/LightSpeed Clean Action Properties	83
Clean/LightSpeed Clean Action Options	84
Appendix C.Actions Add-In Manager	89
Introducing the Actions Add-in Manager	90
Adding New Actions.....	91
Modifying Action Properties	92

Chapter 1: Introducing Workshare Policies

The Workshare Policy Designer provides a central management console where you can configure and manage content security policies. The policies provide control over content electronically leaving your organization and can be distributed to Workshare Protect clients.

This chapter includes the following sections:

- What are Policies?, page 6
- What Policy does Protect Apply?, page 9
- Creating Policies in the Policy Designer, page 13

What are Policies?

Policies are what Workshare Protect uses to check documents for sensitive data. Workshare includes several default policies so without any admin intervention, Workshare can detect and alert to metadata in open documents and email attachments.

However, Workshare is configurable and, using the Workshare Configuration Manager, administrators can adapt and customize how Workshare detects sensitive data and how much input end-users can have over the process.

The Policy Designer extends the possibilities of Workshare further by enabling the customization and creation of policies.

Note: By default, Workshare Protect is configured to work with the Interactive Protect panel and this does NOT use policies at all.

Key points

These are some key points to remember:

- Workshare checks documents against .runtimepolicy files
- .runtimepolicy files are the files that the Policy Designer publishes
- .policy files are the files that the Policy Designer can edit
- Interactive Protect does NOT understand or honour either the .policy or .runtimepolicy files
- Interactive Protect can ONLY be configured (to a limited degree) via the Interactive Protect category in the Administrator mode of the WCM
- The Email Security dialog and the Protect Profile dialog are the only Protect dialogs that understand and honour .runtimepolicy files
- The .runtimepolicy and .policy files that the Policy Designer creates are mostly VERSION SPECIFIC. This means you should use the version of the Policy Designer that corresponds to the version of Professional/Protect that the .runtimepolicy will be used with.

Key terms

A **profile** is a collection of policy sets.

A **policy set** contains one or more policies.

A **policy** includes a condition (if this situation exists) and an action (do this). For example, if the attachment is a Word file and it includes the word “confidential” in the header then block this email if it is sent externally.

What is monitored?

Workshare monitors email attachments and open Office documents for potential policy violations, checking content, context, sender, recipient and channels. Policy actions can be configured to automatically deal with sensitive content by cleaning metadata and hidden data, blocking the email or converting to secure PDF. All policy violations and actions can be visible or hidden to users depending on how they are defined in the policy.

Workshare applies a policy according to the following flow:

1. What channel is the event taking place in? For example, data is being sent by email.
2. What policy set has been defined for this channel?
3. Have any of the conditions defined in the policies in this policy set been satisfied?
4. If so, apply the action defined in that policy, for the specific recipient or specific sender. For example. Block the email when it is sent to users external to your organization and send the email with an alert when it is sent to users within your organization.

Default policies

The installation of Workshare Professional/Protect includes several default policies. Policy sets are installed at:

C:\ProgramData>Workshare

Two folders are created - **Protect Enterprise** and **Policy Sets**. The important one is **Policy Sets**, the other is empty. The **Policy Sets** folder includes the default policy sets provided with Workshare as shown below:

PolicySets	ClientProfiles	Clean	Clean.runtimepolicy LightspeedClean.runtimepolicy
		Clean & PDF	Clean+PDF.runtimepolicy LightspeedClean+PDF.runtimepolicy
		Clean & Secure File Transfer	Clean.runtimepolicy LightspeedClean.runtimepolicy SendLink.runtimepolicy
		Default	WorkshareClient.runtimepolicy
		SecureFileTransfer	SendLink.runtimepolicy
	Send And Protect	Send And Protect Lightspeed.runtimepolicy Send And Protect.runtimepolicy SendLink.runtimepolicy	
	SendLink	SendLink.runtimepolicy	

In addition, the two top level folders - **Protect Enterprise** and **Policy Sets** - are created at:

C:\Users>[user name]>AppData>Roaming>Workshare

In this Users location, the Policy Sets folder includes a subfolder called ClientProfiles. All are empty immediately after install. However, once users make any changes to the default policy via the Workshare Configuration Manager or the Registry, a subfolder called Default is added to the ClientProfiles subfolder and WorkshareClient.runtimepolicy is copied from the ProgramData location to the Users location and updated in the Users location only.

This is important to remember - when users make changes via the Workshare Configuration Manager or Registry, the policy is updated in the Default subfolder in the Users location only.

Example:

*Open the Workshare Configuration Manager and modify any parameter setting, for example in **Protection > Remove Metadata**. Click **Apply**.*

*Look at the date stamp on the WorkshareClient.runtimepolicy file in the **ProgramData** location and compare to the date stamp on the WorkshareClient.runtimepolicy file in the **Users** location. Only the file in the **Users** location is updated.*

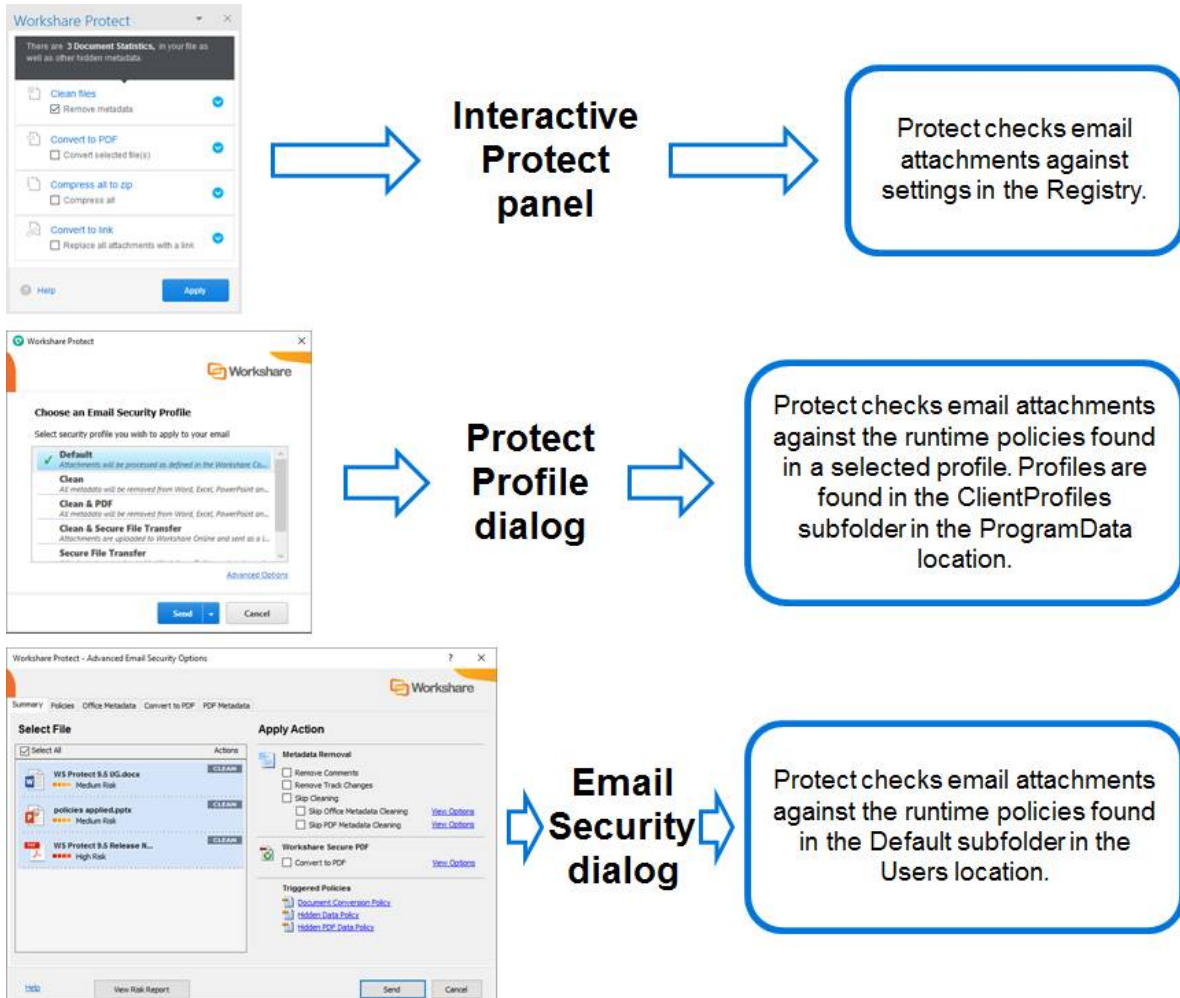
Additionally, a folder is created called **My Policies** at the following location:

C:\Users>[user name]>Documents>My Policies

This is the default save location when saving .policy files in the Policy Designer and the default publish location when selecting to publish .runtimepolicy files for manual distribution.

What Policy does Protect Apply?

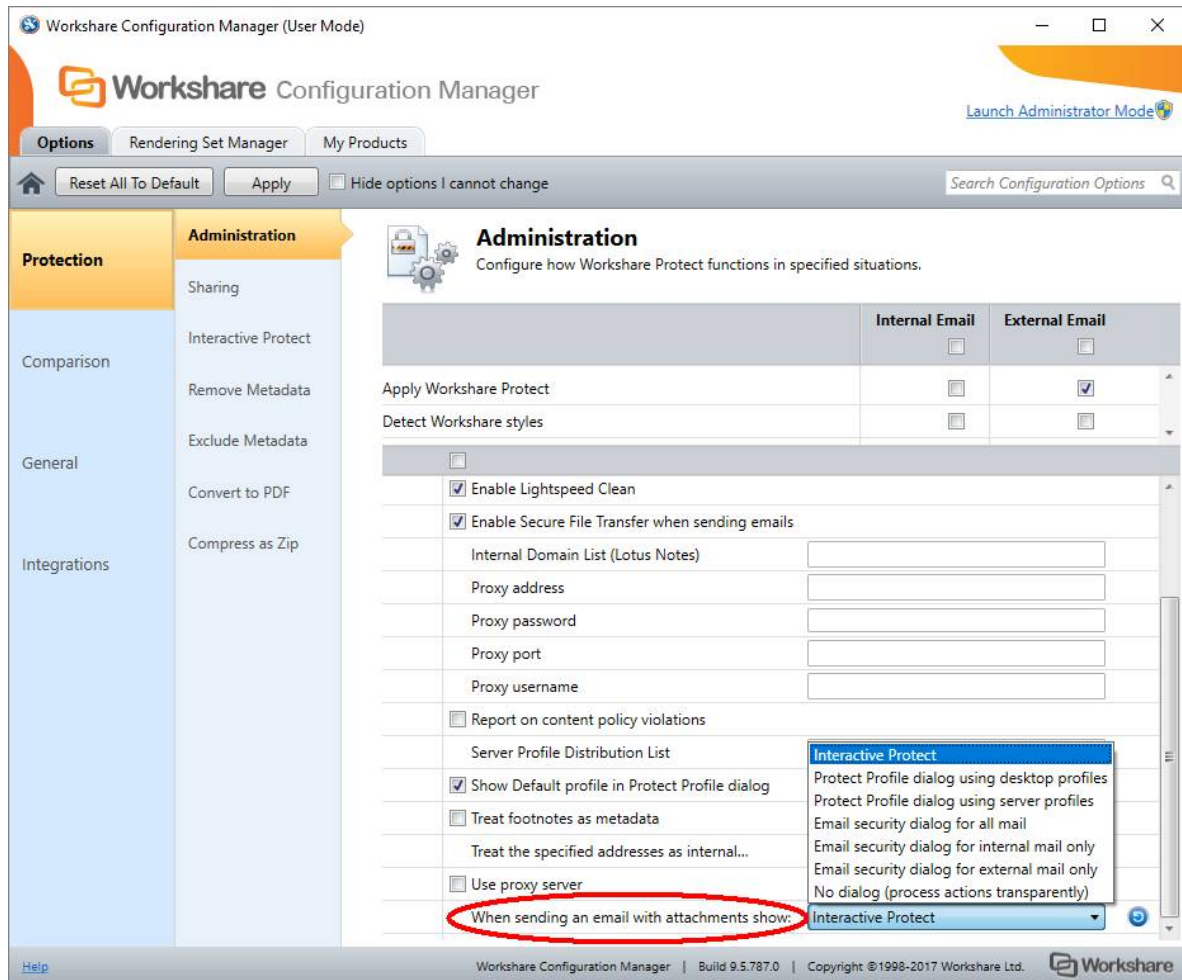
In some situations, Workshare Protect uses policies when checking documents for content risk or metadata. When checking open Microsoft Office documents, Protect always applies the default policy but when checking email attachments, the configuration of Protect determines whether it applies policies and which policies it applies.



If Protect finds a document breaches a policy, it will take the action specified in that policy.

How to configure Protect

Protect is configured in the Workshare Configuration Manager to use the Interactive Protect panel, the Email Security dialog or the Protect Profile dialog. By default, Protect uses the Interactive Protect panel.



Interactive Protect panel (default)

Users see the Interactive Protect panel in their email window as soon as they add an attachment to the email. The panel shows what metadata has been found in the attachments. The user can select what to do with the attachments – clean, convert to PDF, share in a group. You the administrator can set what the default selection should be or you can lock down certain actions so the user has no control. This is done from the Workshare Configuration Manager.

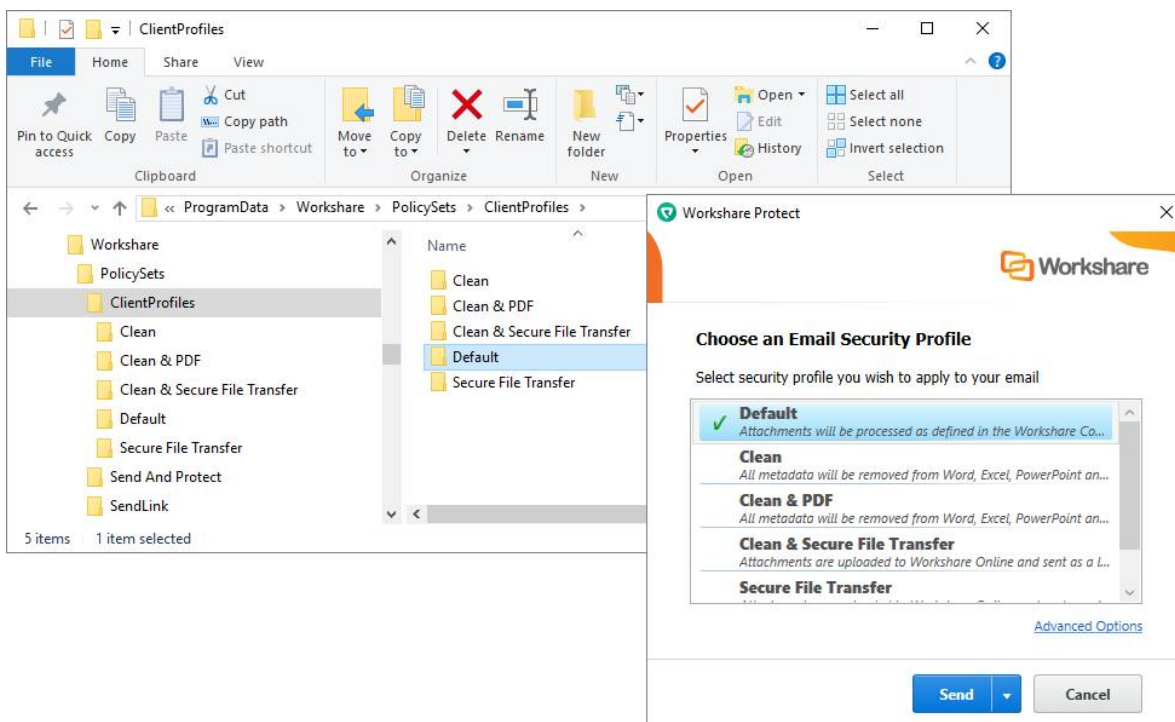
Interactive Protect does NOT use policies at all. It is configured in the Workshare Configuration Manager in the **Protection > Interactive Protect** category.

- Positives....** Interactive Protect is very engaging to use and does not get in the way of the send process. It can be configured to only show what users need, with defaults and to make options visible/invisible to users.
- Negatives....** Interactive Protect is not as extensible and customizable as other options as it does not work on .policy/.runtimepolicy files.

Protect Profile dialog

The Protect Profile dialog enables the user to select from a list of profiles. By default, the user can select **Default**, **Clean**, **Clean & PDF**, **Secure File Transfer** or **Clean & Secure File Transfer**.

The profiles correspond to the names of the subfolders in **ClientProfiles** found at: **C:\ProgramData>Workshare>PolicySets**.



Protect will apply the runtime policies found in the selected profile. In order for a profile to be available in the Protect Profile dialog, it must include at least one .runtime policy file. However, if the user selects the **Default** profile, Protect will look to the **Users** location and apply the runtime policies found in **C:\Users>[user name]>AppData>Roaming>Workshare**.

Example:

Create a new subfolder in **C:\ProgramData>Workshare>PolicySets>ClientProfiles**. Call it “Test Profile”. You will see in the Protect Profile dialog, “Test Profile” will not be an available profile to select.

Now copy a .runtimepolicy file into the “Test Profile” subfolder. You will see in the Protect Profile dialog, “Test Profile” is now an available profile to select.

Positives.... The Protect Profile dialog is useful to apply a collection of policies while ensuring user simplicity. It is good for most users as they can quickly decide which profile to choose based on what they are doing (“Personal”, “Opposing Counsel”, etc.) It provides a good middle ground between usability and customizability.

To modify profiles.....

Use the Policy Designer to modify existing policies or create new policies. **Remember to ensure the .runtimepolicy files published by the Policy Designer are placed in existing or new subfolders in C:\ProgramData>Workshare>PolicySets>ClientProfiles or in the Default subfolder in C:\Users>[user name]>AppData>Roaming>Workshare.**

Email Security dialog

The Email Security dialog alerts users to any breaches of security policies in their attachments. If users have been given permission, they can modify the settings for what will happen to the attachments, for example, change what metadata will be cleaned or select that a particular attachment will be converted to PDF.

With the Email Security dialog configured, Workshare applies the runtime policies found in the default policy set – the **Default** subfolder in **ClientProfiles** in the **Users** location.

If Workshare does not find any .runtimepolicy files in the **Users** location, it will copy over the WorkshareClient.runtimepolicy from the **ProgramData** location. If it does not exist in the Program Data location, Workshare will create it from Registry settings.

Positives.... The Email Security dialog is good for power users and useful if policies need to be super granular and extensive around content and context within the document.

Negatives.... With the Email Security dialog, users have to spend time thinking about what to do and then have the responsibility to do it.

To modify policies.....

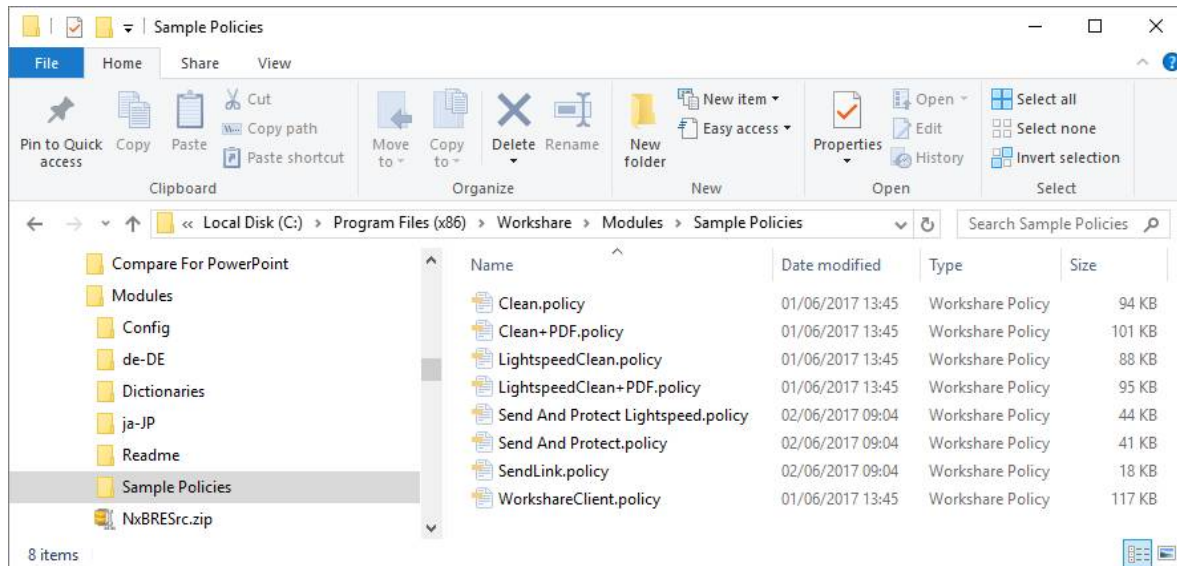
This default policy set can be modified using the Workshare Configuration Manager or the Policy Designer. Making changes in the Workshare Configuration Manager will change the WorkshareClient.runtimepolicy. Using the Policy Designer, you can create new .runtimepolicy files and add them to the Default subfolder. **Remember any .runtimepolicy files in the Default subfolder in the Users location will be applied by Protect.**

Creating Policies in the Policy Designer

Workshare Professional/Protect uses .runtimepolicy files that are smaller in size than those used by previous versions of Professional/Protect. These new-style .runtimepolicy files cannot be opened in the Workshare Policy Designer; ONLY .policy files can be opened in the Policy Designer and modified.

During installation, the .policy files (to match all the default .runtimepolicy files) are placed in the install location. By default, this is:

C:\Program Files (x86)>Workshare>Modules>Sample Policies



You can use the Policy Designer to:

- Create new .policy files
- Edit existing .policy files
- Perform a save as on existing policy files and tweak according to your requirements

Whichever you do, remember:

- **If working with the Email Security dialog, publish .runtimepolicy files to the Default subfolder in the Users location**
- **If working with the Protect Profile dialog, publish .runtimepolicy files to an existing profile or a new profile subfolder in ClientProfiles in the ProgramData location OR to the Default subfolder in the Users location**

It is recommended that you do not modify the WorkshareClient.policy file. If you do modify this default policy, you must ensure that the **Enable automatic generation of default profile** parameter is NOT selected in the **Protection > Administration** category of the Workshare Configuration Manager (Administrator mode). If this is selected, the default policy will be automatically regenerated and the customized settings will be overwritten.

	Content risk runtime policy path (this overrides the default path)	
	<input checked="" type="checkbox"/> Display Advanced Options	
	<input checked="" type="checkbox"/> Display progress bar on Send	
	<input type="checkbox"/> Display Send with Protect button (Outlook)	
	<input checked="" type="checkbox"/> Enable automatic generation of default profile	
	<input checked="" type="checkbox"/> Enable Lightspeed Clean	
	<input checked="" type="checkbox"/> Enable Secure File Transfer when sending emails	
	Internal Domain List (Lotus Notes)	
	Proxy address	
	Proxy password	
	Proxy port	
	Proxy username	

The WorkshareClient.runtimepolicy file is automatically generated from the Registry in the following scenarios:

Action	Location of WorkshareClient.runtimepolicy
Workshare Installation	ProgramData/Workshare/PolicySets/ClientProfiles/Default
Re-running the Workshare Configuration Assistant	ProgramData/Workshare/PolicySets/ClientProfiles/Default
Applying changes in Administrator Mode of the Workshare Configuration Manager	ProgramData/Workshare/PolicySets/ClientProfiles/Default
Applying changes in User Mode of the Workshare Configuration Manager	Users/[current user]/AppData/Roaming/Workshare/PolicySets/ClientProfiles/Default
Changing Registry values in the Registry which correspond to the Protection category options	Users/[current user]/AppData/Roaming/Workshare/PolicySets/ClientProfiles/Default

Note: Publishing a policy in the Policy Designer creates a .runtimepolicy file. You must also save the .policy file as a .policy file.

Chapter 2: Installing the Policy Designer

This chapter describes how to install the Policy Designer. It includes the following sections:

- Installation Overview, page 16
- Upgrading from Earlier Versions, page 16
- Running the Install, page 17

Installation Overview

You must install the version of the Policy Designer that corresponds to your version of Professional/Protect. For example, if you install the 787 build of Professional, you must install the 787 build of the Policy Designer.

The Policy Designer executable is available from Workshare Customer Support.

Upgrading from Earlier Versions

When you are upgrading Workshare Professional/Protect from earlier versions, Workshare replaces the previous default policies at C: Program Data/Workshare with the new default policies.

If you have created your own policy sets using the Policy Designer, you do not need to delete them before upgrading. Workshare will not delete them.

Tip! *You may want to back up your policy sets before upgrading as a precautionary measure.*

However, if you have modified the Workshare default policy sets, then you should save them to another location and copy them back over after the upgrade.

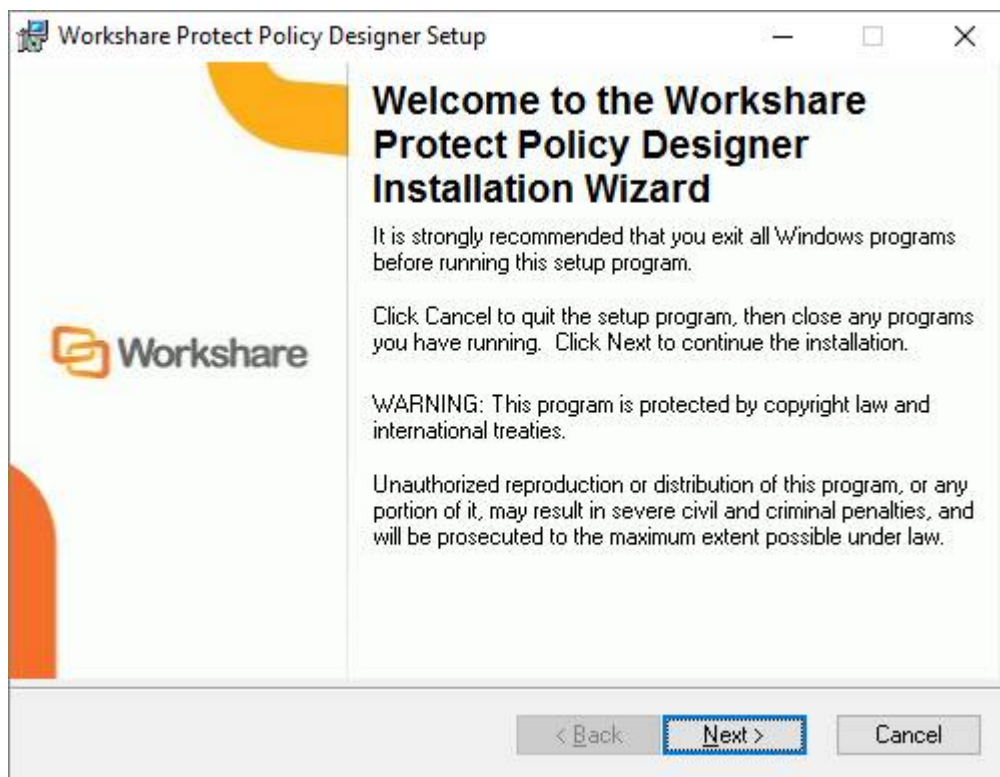
Note: *The WorkshareDocumentRestrictions.runtimepolicy, WorkshareInternal.runtimepolicy and ReadyRedline.runtimepolicy from earlier versions of Professional/Protect MUST be manually removed as they may inhibit the correct working of Professional/Protect 9.5 and above.*

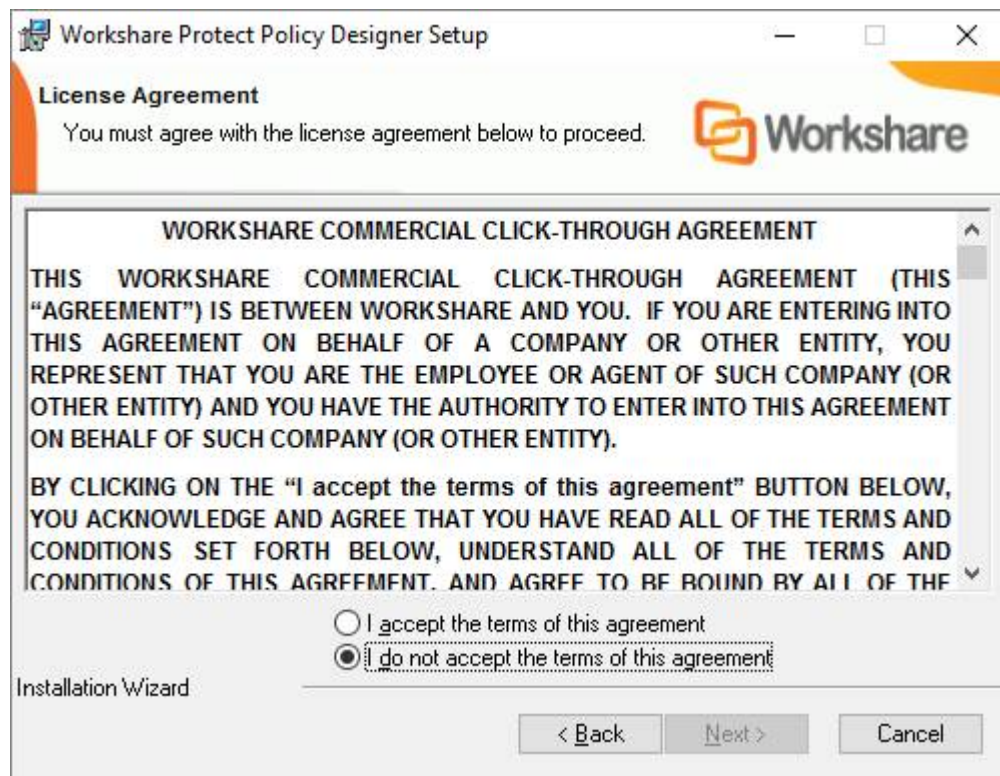
Running the Install

This procedure describes how to install the Workshare Policy Designer by running the executable.

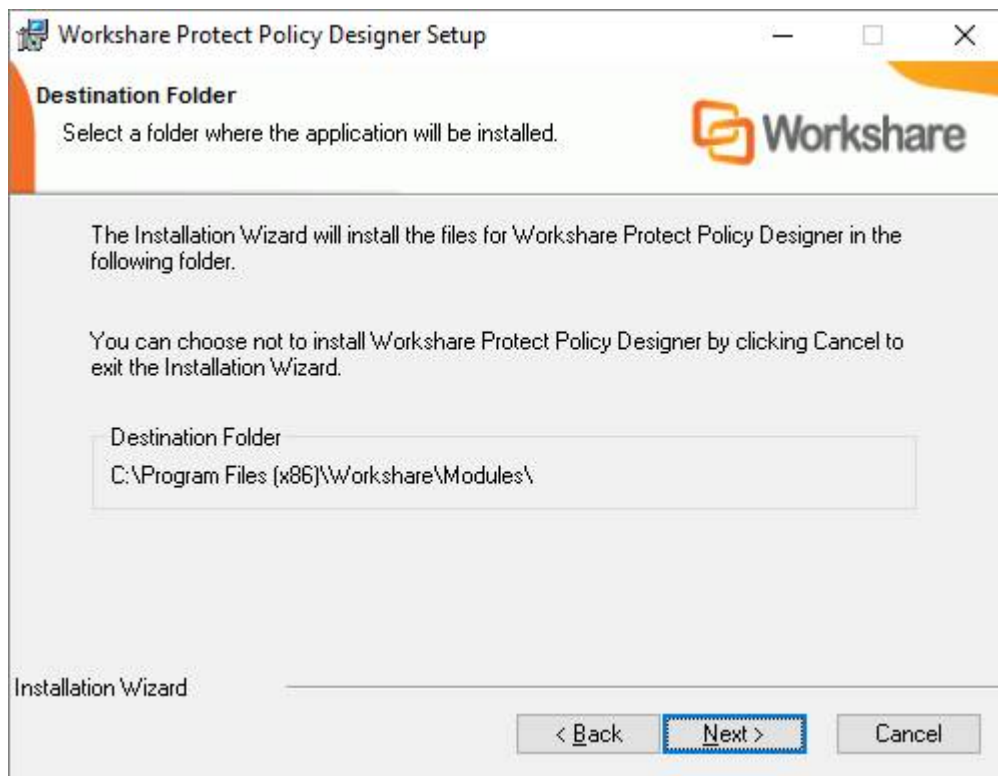
To install the Policy Designer:

1. Double-click WorksharePolicyDesigner-XXX.exe.



2. Click **Next**.

3. Select the **I accept....** radio button and click **Next**.



4. Click **Next**.
5. Click **Next** again and the Policy Designer is installed.
6. Once the installation process is complete, click **Finish**.

Chapter 3: Quick Tour of the Policy Designer

This chapter provides an overview of the Policy Designer interface. It includes the following sections:

- Accessing the Workshare Policy Designer, page 21
- Workshare Policy Designer Main Window, page 22

Accessing the Workshare Policy Designer

Once the Workshare Policy Designer is installed and licensed on your machine, you access it from the desktop or the Start menu.

Note: *The Workshare Policy Designer may only be run by users with administrative privileges.*

To start the Workshare Policy Designer:

Double-click the Workshare Policy Designer shortcut icon on the desktop, or from the Start menu, select **Workshare Policy Designer**. The Policy Designer main window is displayed.






Workshare Policy Designer Main Window

This section describes the functionality of the toolbar icons and menu options in the Policy Designer window.

Toolbar icons

The Policy Designer toolbar contains the following icons:

	New	Enables you to create a new policy set.
	Open Local Policy Set	Enables you to open an existing policy set that has been saved locally.
	Save	Enables you to save the open policy set.

File menu

The File menu contains the following options:

Option	Description
New Policy Set	Enables you to create a new policy set for Active Content and Client Email channels.
Open Policy Set(s)	Enables you to open an existing policy set, including the default policy set, from the local machine.
Recently Opened Policies	Enables you to view and open recently opened policy sets.
Save	Saves the current policy set.
Save As	Enables you to save the current policy set under a different name.
Save All	Saves all open policy sets.
Close	Closes the current policy set.
Publish	Enables you to publish the current policy set.
Unpublish	Enables you to unpublish the current policy set if it has already been published.
Delete	Enables you to delete the current policy set.

Option	Description
Language resource file	<p>Enables you to translate policies into different languages. There are two sub-options as follows:</p> <p>Save file: This sub-option enables you to export a language file from an existing policy set and save it to a location from where it can be translated into another language and then imported back into the policy set.</p> <p>Load file: This sub-option enables you to import a language file that has previously been exported from an existing policy set, saved to a location and translated into another language.</p>
Exit	Closes the Workshare Policy Designer. You are prompted to save any currently open policy sets before exiting

Edit menu

The *Edit* menu contains the following options:

Option	Description
Cut	Enables you to cut a policy file. A cut policy file can be pasted into another policy set or deleted.
Copy	Enables you to copy a policy file. A copied policy file can be pasted into another policy set.
Paste	Enables you to paste cut or copied policy files to new policy sets. The copy/paste functionality provides a quick way to duplicate a policy where you need to tweak a setting.

Tools menu

The *Tools* menu contains the following option:

Option	Description
Add-in Manager	Includes the sub-option Actions that enables you to edit existing actions in the Workshare Policy Designer. For more information about the Add-in Manager, refer to <i>Appendix D: Actions Add-In Manager</i> .

Windows menu

The Windows menu contains the following options:

Option	Description
Cascade	Displays all the open windows in the Workshare Policy Designer so that each window title bar is visible.
Tile Vertical	Displays all the open windows side by side vertically in the Workshare Policy Designer.
Tile Horizontal	Displays all the open windows side by side horizontally in the Workshare Policy Designer.
Dock All	Displays all the open windows on top of each other in the Workshare Policy Designer.
Close All	Closes all the open windows in the Workshare Policy Designer.

***Note:** The Windows menu also displays a list of (and provides access to) the currently opened policy sets.*

Help menu

The Help menu contains the following options:

Option	Description
Contents	Provides access to Workshare Policy Designer online help.
About Workshare Policy Designer	Displays version information about Workshare Policy Designer.

Language settings

When a policy set is open there is a **Select Policy language** dropdown list in the top right of the Policy Designer window. If the policy set is available in other languages, you can change the display language in the Policy Designer by selecting the language from the **Select Policy language** dropdown list. For more information, refer to *Chapter 8: Language Files*.

Chapter 4: Policy Sets and Policies

This chapter describes how to set up and maintain policy sets and policies. It includes the following sections:

- Creating Policy Sets, page 26
- Creating New Policies, page 30

Creating Policy Sets

A policy set is a group of related policies. You can distribute policy sets across a network or to a standalone computer and Workshare Protect uses the policies contained in the policy set to secure data and stop information security breaches. A policy set is defined for a particular channel – email or open Office documents (active content).

Terms and concepts

These are the terms used in the Workshare Policy Designer when creating policies:

- **Policy:** Policies are a set of rules and guidelines to ensure employee best practice when distributing information. Policies are defined by a condition (consisting of one or more expressions) and an action that is executed when the condition is met.
- **Policy Set:** A policy set is a group of related policies.
- **Condition:** A condition specifies the circumstances that must exist in order for Workshare Protect to detect data as sensitive. A condition is a collection of one or more expressions. Where multiple expressions exist, they are related by **AND** or **OR**.
- **Expression:** An expression specifically defines what content in what context is considered sensitive.
- **Channel:** A channel is the way in which information is distributed, for example, by email.
- **Routing:** Routing is a method of identifying privileged and non-privileged senders of information and trusted and non-trusted receivers of information. When defining policies that cover emails and email attachments, you can specify actions according to senders and receivers.
- **Action:** Actions specify what should happen once a condition has been met, for example, block, alert, clean, PDF.

Building a policy

Workshare Protect detects sensitive information according to the *policy set*. A policy set can include one or more policies. A *policy* determines what information Workshare Protect will detect as sensitive and specifies what action Workshare Protect will take when it detects sensitive information sent to specific recipients/destinations or from specific senders. A policy defines the *condition* that must exist in order for Workshare Protect to detect data as sensitive and the *action* that should be taken when the condition is met. A condition is made up of *expressions* that define what content is considered sensitive. A condition can include one or more expressions. Actions can be specified according to sender/source and receiver/destination.

Policy sets are defined based on *channels*. A channel is the way in which information is distributed. Workshare Protect monitors traffic that uses the following channels:

- **Client Email:** Emails and their attachments
- **Active Content:** Open Microsoft Office documents

Note: *Active Content policies (that are applied to open Microsoft Office documents) are not defined according to sender/receiver or source/destination.*

For example, you may define a policy as follows: Confidential Information Policy for Client Email:

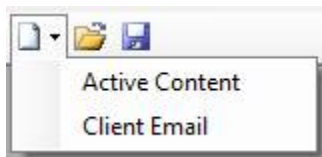
- **Condition:** When an attachment is a Microsoft Word, Excel or PowerPoint document that includes the words “Private and Confidential,” perform the following actions:
- **Actions:** Perform a Block action when the email is sent from user group A to user group B and an Alert action when the email is sent from user group A to user group C.

Creating a new policy set

This procedure describes how to create a policy set from scratch.

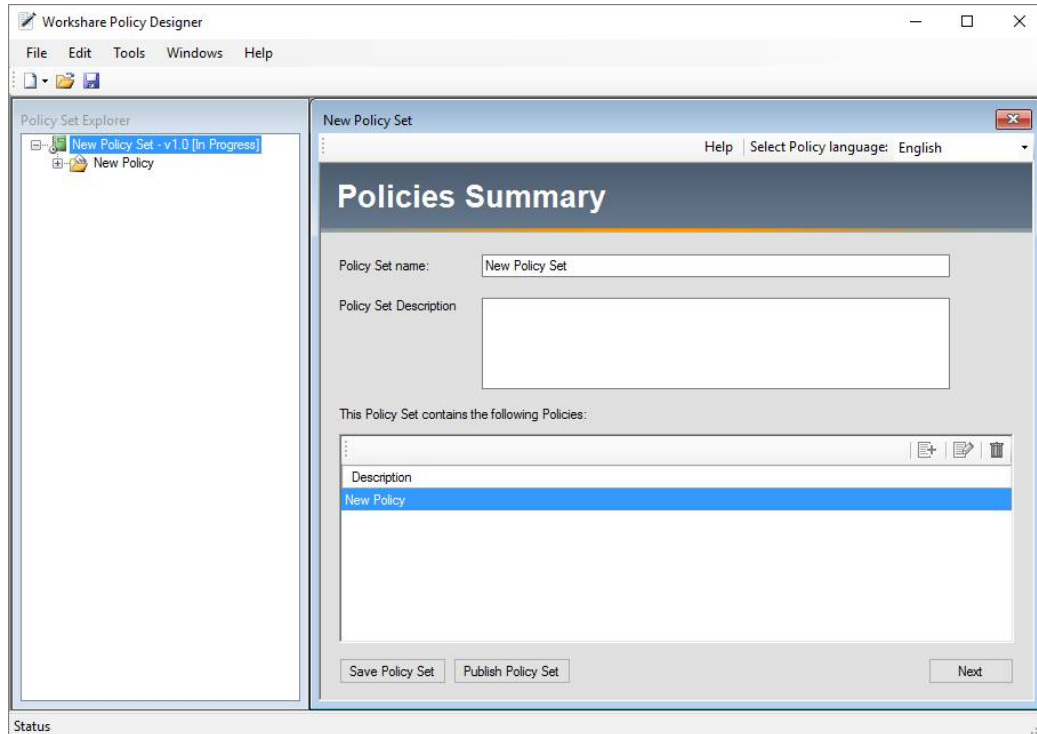
To create a new policy set:


1. In the Policy Designer main window, click the **New** icon or from the *File* menu, select **New Policy Set**.

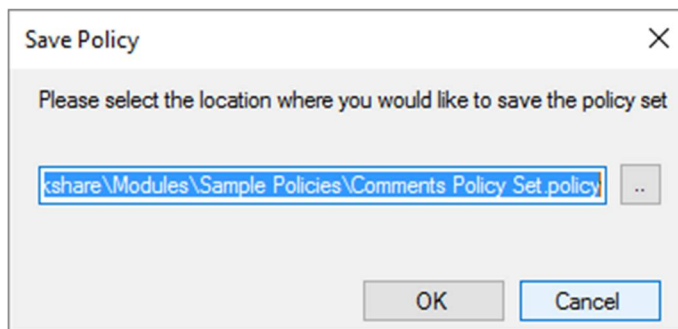


2. Select the channel that you want the policy set to apply to.

The *Policies Summary* window is displayed in the right-hand pane and the Policy Set Explorer tree is displayed in the left-hand pane of the Policy Designer main window. By default a single policy (called **New Policy**) is included in the new policy set.



3. Enter a name for the policy set in the **Policy Set name** field. The name is displayed in the Policy Set Explorer tree.
4. Click the  icon, select **Save** from the *File* menu or click **Save Policy Set** in the *Policies Summary* window. The *Save Policy* dialog is displayed.



5. Click **OK** to save the policy set in the default local location (**Program Files\Workshare\Modules\Sample Policies**) as a .policy file. To change the location, enter a different location or click the browse button and select a different location.

You can now edit the default policy included in the policy set and create new policies. For more information, refer to *Creating New Policies*, page 30.

Opening the default and existing policy sets

You can open policy sets that you have saved as well as the default policy sets. You can only open .policy files in the Policy Designer.

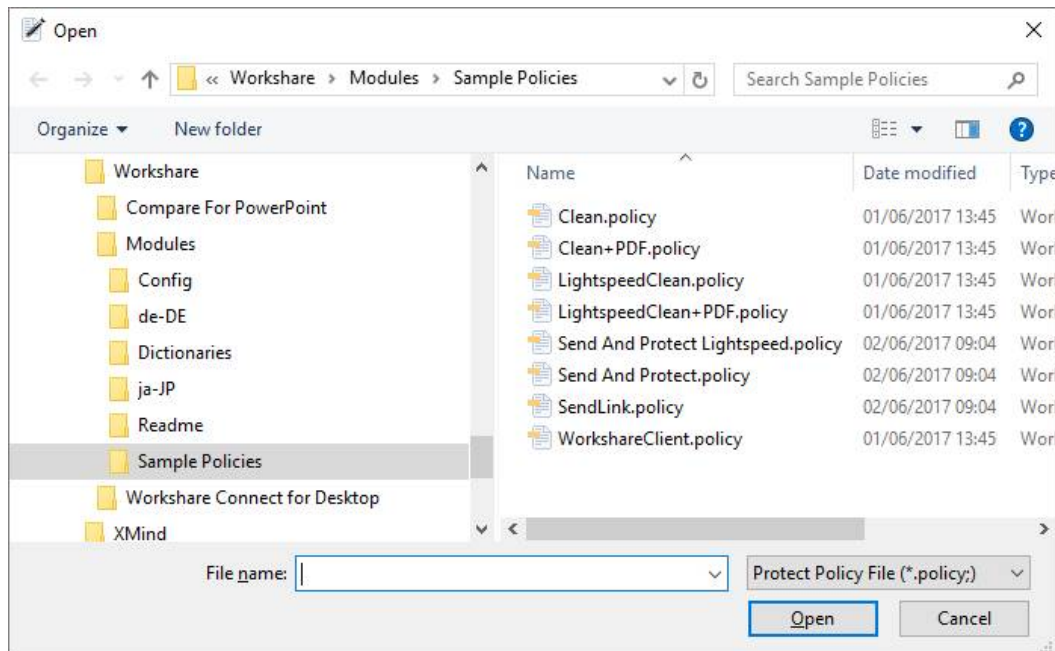
Note: .runtimepolicy files are the files that the Policy Designer publishes and .policy files are the files that the Policy Designer can edit.

During installation of Workshare Professional/Protect, the .policy files (to match all the default .runtimepolicy files) are placed in the install location. By default, this is C:\Program Files (x86)>Workshare>Modules>Sample Policies.

You can open these default .policy files, edit them and publish them to the default location so that they replace the existing default .runtimepolicy files.

To open a policy set:

1. In the Policy Designer main window, click the  icon or from the *File* menu, select **Open Policy Set(s)**. The *Open* dialog is displayed. The default location is the **Program Files\Workshare\Modules\Sample Policies** folder.




2. Select one or more policy sets and click **Open**. To select multiple policy sets, hold the Shift or Ctrl keys. You can select the default policy set or a previously saved custom policy set from the **My Policies** folder or you can browse to a different location where you have previously saved a custom policy set. A policy set has the extension **.policy**.
3. Click **Open**. The selected policy set is opened in the Workshare Policy Designer.

Creating New Policies

Policies are composed of rules and guidelines to ensure employee best practice when distributing information. A policy determines what information Workshare Protect will detect as sensitive and specifies what action Workshare Protect will take once it detects sensitive information. A policy defines the conditions that must exist in order for Workshare Protect to detect data as sensitive and the actions that should be taken when the conditions are met. Multiple policies can exist within a policy set.

To create a new policy:

1. Click **Next** in the *Policies Summary* window after creating a new policy set or open an existing or new policy set and in the Policy Set Explorer tree, right-click the policy set and select **Add Policy**. The *New Policy* window is displayed in the right-hand pane of the Policy Designer window.



Policy

POLICY DETAILS

The following descriptions will be displayed when the Policy is triggered.

Short Description:


New Policy

Long Description:

☒ Block On Execution Error

Back Next

2. In the **Short Description** field, enter a relevant name for the policy. This name is displayed in the Policy Set Explorer tree and is also displayed in the *Workshare Protect Email Security* dialog to provide a description of the policy for the user.
3. In the **Long Description** field, enter a concise summary of the policy to define the function of this policy. This is also displayed in the *Workshare Protect Email Security* dialog to provide an explanation for the user.

4. Select the **Block On Execution Error** checkbox to trigger a Block action in the event that the original action fails.
5. Click the  icon or select **Save** from the *File* menu. The policy is saved to the policy set.

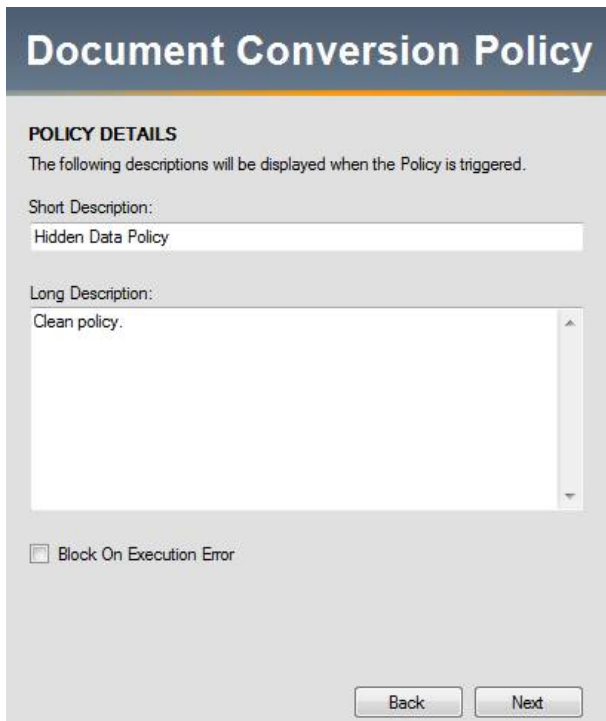
You can now define conditions for this policy by clicking **Next**. For more information, refer to *Chapter 5: Conditions and Expressions*.

Viewing and Editing Existing Policies

You can view and edit details for all existing policies in a policy set.

To view the details of an existing policy:

1. Open the policy set containing the policy that you want to view.
2. Select the policy in the Policy Set Explorer tree. The details of the selected policy are displayed in the *Policy* window in the right-hand pane of the Policy Designer window.



Document Conversion Policy

POLICY DETAILS
The following descriptions will be displayed when the Policy is triggered.

Short Description:
Hidden Data Policy

Long Description:
Clean policy.

☐ Block On Execution Error

Back Next

3. Edit the **Short Description**, **Long Description** and other settings of the policy as required. You can also view the conditions contained within the policy by clicking **Next**. For more information, refer to *Viewing and Editing Existing Expressions*, page 37.
4. Save the open policy set.

Copying Policies

You can copy policies from one policy set to another in the Policy Set Explorer tree by selecting **Edit > Copy** (or Ctrl+ C) and pasting the policy to the desired policy set using **Edit > Paste** (or Ctrl + V). The policy will also remain in its original policy set.


Deleting Policies

This section describes how to delete policies from a policy set.

To delete a policy:

1. Open the policy set containing the policy that you want to delete.
2. Select the policy that you want to delete in the policy list in the *Policies Summary* window.

The screenshot shows the 'Policies Summary' window. At the top, the title is 'Policies Summary'. Below it, there are two fields: 'Policy Set name:' with the value 'Comments Policy Set' and 'Policy Set Description:' with the value 'Includes policies to delete different types of comments from Office files'. Below these fields, it says 'This Policy Set contains the following Policies:'. There is a list of policies: 'Description', 'Comments Policy', 'Track Changes Policy', and 'Footnotes Policy'. The 'Footnotes Policy' is highlighted in blue. To the right of the list, there are three icons: a plus sign, a pencil, and a trash can. At the bottom of the window, there are three buttons: 'Save Policy Set', 'Publish Policy Set', and 'Next'.

3. Click the **Delete the selected Policy**  button. A confirmation prompt is displayed.
4. Click **Yes** to delete the policy, or click **No** to cancel. The policy is deleted from the policy set.

Note: To delete a policy, you can also right-click the policy that you want to delete in the Policy Set Explorer tree and select **Delete this Policy**.

Chapter 5: Conditions and Expressions

This chapter describes how to define a condition by specifying expressions. It includes the following sections:

- Defining Conditions, page 34
- Configuring Expressions, page 39

The procedure for defining conditions and expressions is the same regardless of to which channel the policy applies.

Defining Conditions

A condition specifies the content that Workshare Protect detects. A condition is a collection of one or more expressions that define what content is considered sensitive. There is only one condition within a policy but there can be multiple expressions within that condition. When multiple expressions exist within a condition, the Policy Designer uses the following expression logic:

- **And:** Use this if you want to add multiple expressions to a condition and you want all the circumstances defined by the expressions to exist in order for the condition to be met (for example, if X and Y occur, the condition is met).
- **Or:** Use this if you want to add mutually exclusive expressions to a condition so that as long as the circumstances defined in one of the expressions exist, the condition is met (for example, if X or Y occurs, the condition is met).

To define a condition:

1. In the Policy Set Explorer tree, select the policy into which you want to add a new condition.
2. Click **Next**. The *Condition* window is displayed in the right-hand pane of the Policy Designer window.

Comments Policy Set

Help | Select Policy language: English

Condition

POLICY CONDITION SET

Active Expressions:

Logic: AND

Expression Details

The following descriptions will be displayed when the selected Expression is triggered:

Short Description:

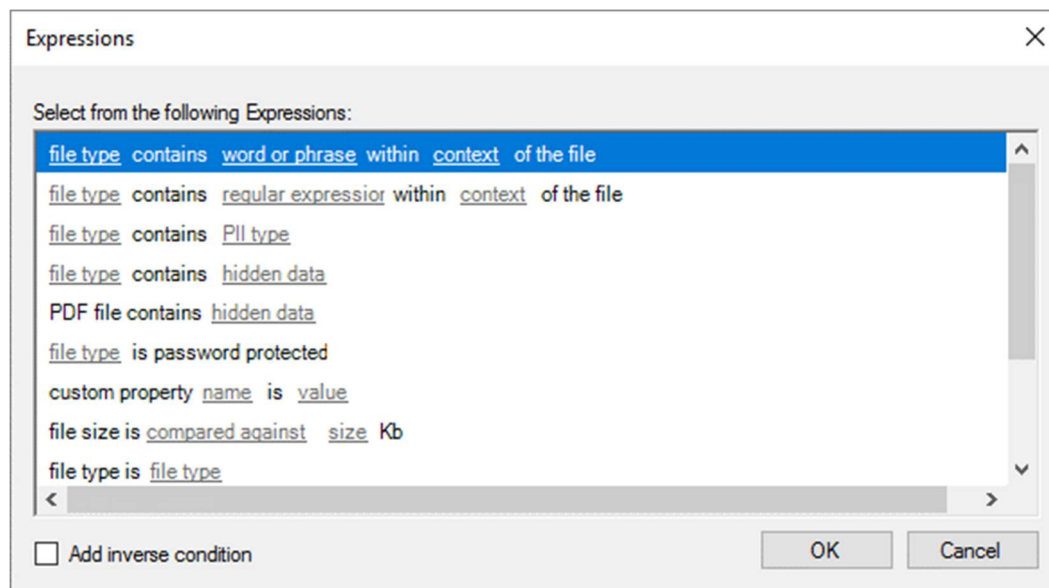
Long Description:

Risk Rating:

Back Next

Tip: You can also expand the policy in the Policy Set Explorer tree and select **Condition**.

3. Click the **Add a new Expression**  button. The *Expressions* dialog is displayed.



Note: For detailed information about configuring expressions, refer to *Configuring Expressions*, page 38.

4. Select the expression that you want to add to the condition and click **OK**.
5. If you want to add the inverse of the condition, select the **Add inverse condition** checkbox before clicking **OK**. This means that instead of the expression being, for example, “Word document is password-protected”, it is “Word document is NOT password-protected”.

Warning: The NOT operator negates the entire condition and conditions using it should be thoroughly tested to ensure results are as intended. For example, in the example given above, any email will trigger the condition. To ensure the condition is triggered only by MS Word documents, you must add another expression saying that “File Type is Word” and link the two expressions using the AND operator. This will ensure the required result that non-password-protected Word documents trigger the condition.

6. Quantify the expression by clicking the blue underlined links and specifying the parameters for the expression. For more information, refer to *Configuring Expressions*, page 38.

Note: You *must* add a value for each of the underlined links for an expression to be valid. If you do not, you will not be able to save or publish the policy.

- In the **Short Description** field, enter a short description for the expression to give a brief summary of what you have set this expression to do. This is displayed in the *Workshare Protect Email Security* dialog to provide an explanation for the user as to what triggered the policy.

Note: You *must* add a description in the **Short Description** field for an expression to be valid. If you do not, you will not be able to save or publish the policy.

- In the **Long Description** field, enter a longer description for the expression to provide more information on the exact functionality of the expression. This is displayed in the *Workshare Protect Email Security* dialog to provide an explanation for the user as to why the policy is important.
- From the **Risk Rating** dropdown list, select the expression risk rating (**High**, **Medium** or **Low**).

The screenshot shows a software window titled "Comments Policy Set". At the top, there is a "Help" link and a "Select Policy language: English" dropdown. The main heading is "Condition". Below this, the "POLICY CONDITION SET" section shows "Active Expressions:" with a list containing "any file type contains Comment". To the right, the "Expression Details" section provides fields for "Short Description:" (containing "Office file contains comments"), "Long Description:" (an empty text area), and "Risk Rating:" (a dropdown menu currently set to "High"). At the bottom of the main area are "Back" and "Next" buttons.

10. Optionally repeat steps 3 to 9 to add further expressions to the condition. When adding multiple expressions, select the appropriate expression logic (either **AND** or **OR**) from the **Logic** dropdown list. (This is defaulted to **AND**.)



11. Click the  icon or select **Save** from the *File* menu.

You can now assign actions to the condition by clicking **Next**. For detailed information about adding actions, refer to Chapter 6: *Channels and Action Sets*.

Viewing and editing existing expressions

This section describes how to view and edit the details for existing expressions.


To view the details of an existing expression:

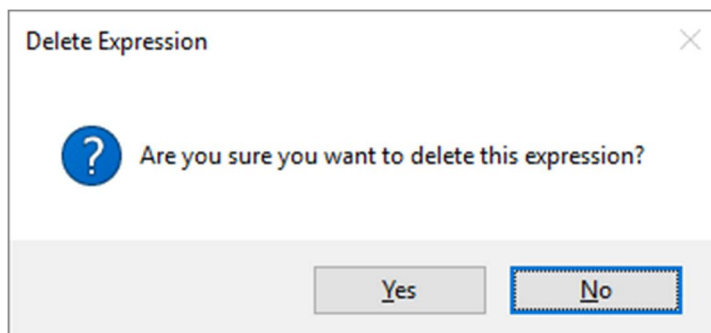
1. Expand the policy you want to view or modify in the Policy Set Explorer tree and select **Condition**.
2. The expressions for that particular condition are displayed in the center pane. Expressions can be edited by clicking the blue underlined links. Additionally, you can also edit the **Short Description**, **Long Description**, and **Risk Rating** fields. Further expressions can be added to the condition by clicking the **Add a new Expression**  button.
3. Click the  icon or select **Save** from the *File* menu.

Deleting expressions

This section describes how to delete expressions from a condition.

To delete an expression:

1. Select the expression that you want to delete in the center pane of the *Condition* window.
2. Click the **Delete the selected Expression**  button. The following prompt is displayed.



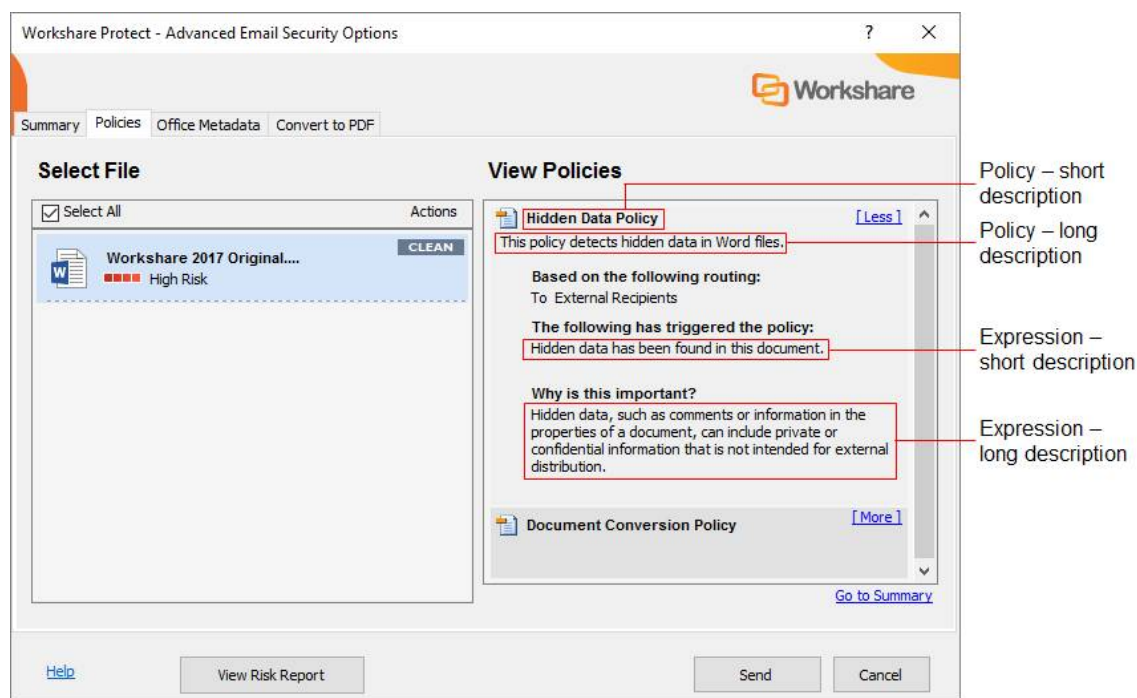
3. Click **Yes** to delete the expression. The expression is deleted from the condition.

Note: You must save the open policy set before closing it to ensure that this expression is permanently deleted from the policy set.

What users see

The names and descriptions for policies and expressions are visible to the user as follows:

In the Advanced Email Security Options dialog:



Configuring Expressions

When quantifying expressions, you specify the parameters of the expression by clicking the blue underlined link. Different dialogs are displayed according to the link selected. Details of each link and expression parameters are provided in this section.

Rules about expressions

You should be aware of the following basic rules when configuring expressions.

1. When configuring file type expressions (expressions that include a “**file type**” link), do not add multiple expressions that specify different file types and use the AND expression logic. This will result in an error when the policy set is published.

For example:

Word file contains **Private** within **Any Context** of the file

AND

Excel file contains **Confidential** within **Cell Text** of the file

This combination of different file types together with the AND logic means that Workshare Protect will look for a document that is both a Word file and Excel spreadsheet, which is not possible.

2. You cannot add two conflicting expressions, for example, an expression that specifies a file size greater than 10 kb and an expression that specifies a file size less than 10 kb.
3. Where an expression includes a “**file type**” link, some of the available actions will not apply to all file types and an error message will display.

For example:

If you select **Email** as a file type along with a **PDF**, **LightSpeed Clean**, **PDFClean** or **Zip** action, the action will not be carried out as email files cannot be converted to PDF, cleaned or zipped. If expressions contain this type of inconsistency, one of the following error messages will display:

- When the condition set includes some file types for which the action can apply (for example, email and Microsoft Word files), a warning will indicate which file types are not compatible with the action.
- When the condition set includes only file types for which the action does not apply, for example, Email, RTF and HTML, an error displays and the policy set cannot be published.

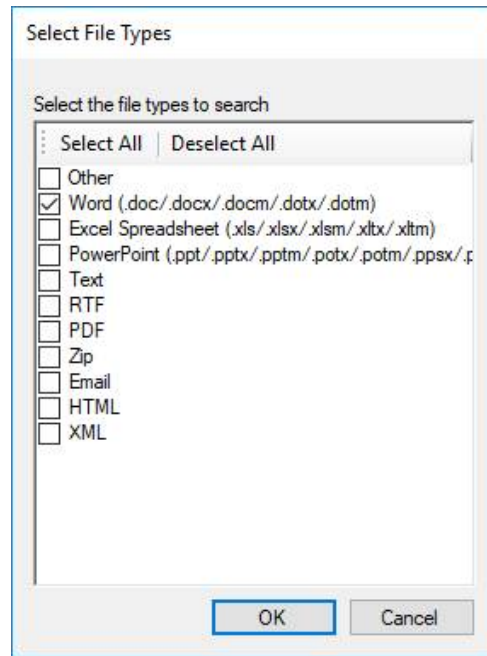
file type contains word or phrase within context of the file

This expression specifies that if Workshare Protect finds a specified word or phrase within a specified area of a specified file type, then the condition will be met. Example: A Microsoft Word or Excel document contains the word “confidential” in the header or footer.

File type

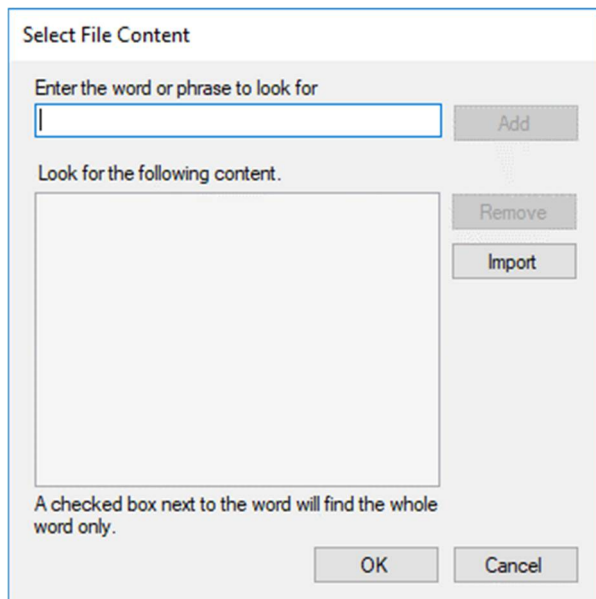
Clicking the expression link displays the *Select File Types* dialog.

Select the file type(s) that you want the expression to cover and click OK. You can use the Select All and Deselect All buttons to aid you in the selection of the different file types.



Word or phrase

The **Word or phrase** link enables you to specify the word or phrase (for example, “confidential”, “restricted” or profanity) that Workshare Protect should identify as sensitive information. Clicking the **word or phrase** expression link displays the *Select File Content* dialog.



Enter the word(s) or phrase(s) required to trigger the expression in the **Enter the word or phrase to look for** field. Click **Add** to move it to the **Look for the following content** list.

Items added to the list are checked by default. When items are checked, Workshare Protect searches for the whole word or phrase. Uncheck the box next to any words or phrases to search for partial matches.

To delete word(s) or phrases from the list, select the word or phrase and click **Remove**.

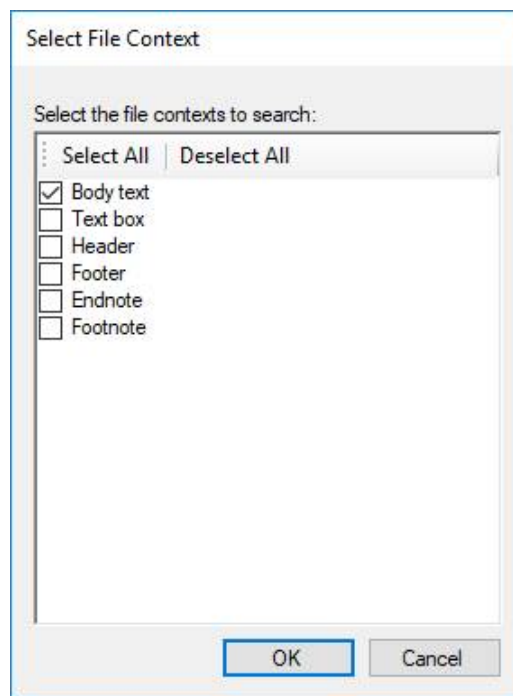
Click **Import** and select a text file that includes the content to be identified as sensitive information

Click **OK** to save your changes.

Context

The **context** link enables you to specify the elements of a document where Workshare Protect should look for sensitive information. Clicking the **context** expression link displays the *Select File Context* dialog.

Select the area of the document where the word or phrase may appear by clicking the corresponding checkboxes and click OK. You can use the Select All and Deselect All buttons to aid you in the selection of the different file contexts.



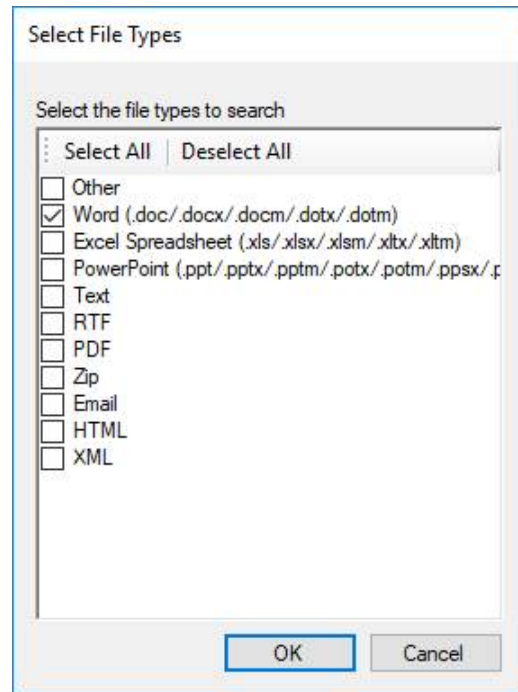
file type contains regular expression within context of the file

This expression specifies that if Workshare Protect finds a specified expression within a specified area of a specified file type, then the condition will be met. Example: A Word document contains a regular expression within the body text.

File type

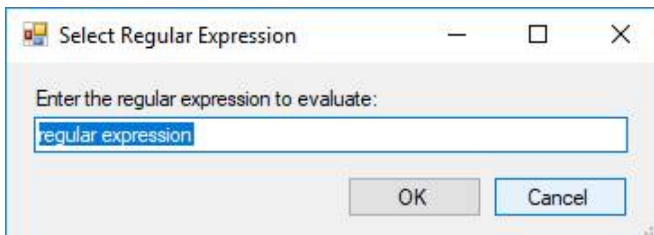
Clicking the **file type** expression link displays the *Select File Types* dialog.

Select the file type(s) that you want the expression to cover and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file types.



Regular expression

The **regular expression** link provides a way of matching text that follows a particular pattern, according to certain rules. A regular expression is a special text string for describing a search pattern and is used to give a concise description of search parameters without having to list all the prospective matches. Clicking the **regular expression** link displays the *Select Regular Expression* dialog.



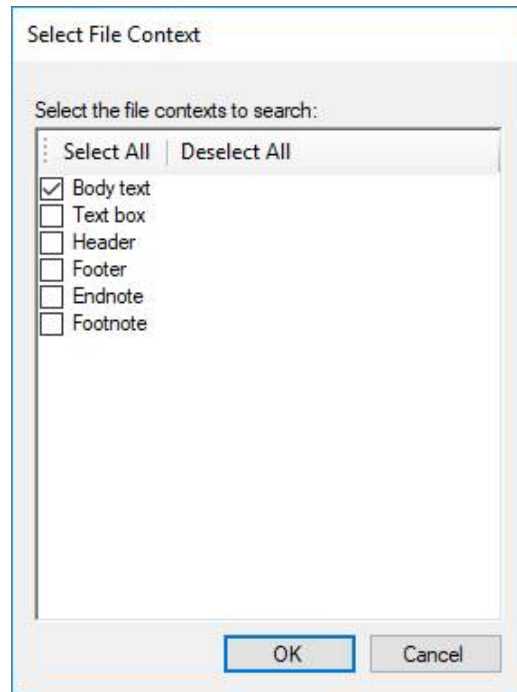
Enter the relevant code string describing the particular search pattern required to trigger the expression and click **OK**.

Note: More information on creating regular expressions can be found in Appendix B: Regular Expressions.

Context

Clicking the **context** expression link displays the *Select File Context* dialog.

Select the area of the document where the regular expression may appear by clicking the corresponding checkboxes and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file contexts.



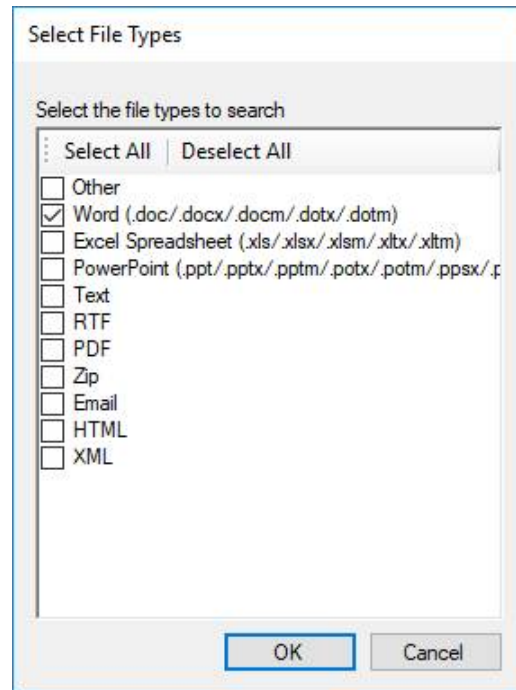
file type contains PII type

This expression specifies that if Workshare Protect finds that a file type that contains a specified PII type (Credit Card or Social Security Number), then the condition will be met. Example: A Word file contains Credit Card and Social Security Number.

File type

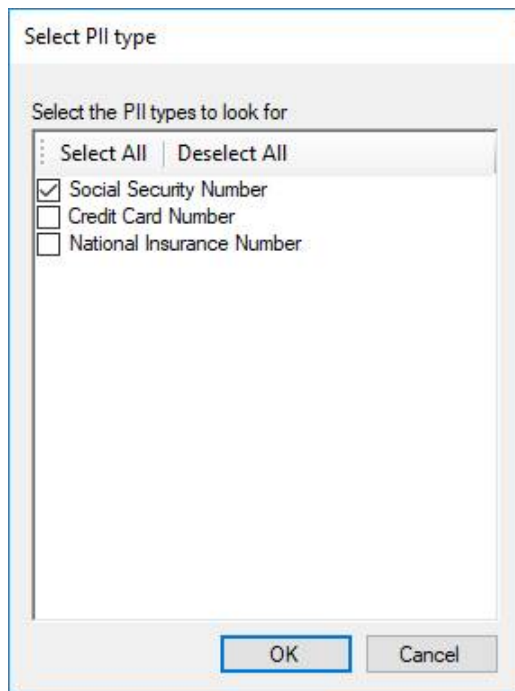
Clicking the **file type** expression link displays the *Select File Types* dialog.

Select the file type(s) that you want the expression to cover and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file types.



PII type

Clicking the **PII type** expression link displays the *Select PII type* dialog.



Select **Social Security Number** and/or **Credit Card Number** and/or **National Insurance Number** and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different PII types.

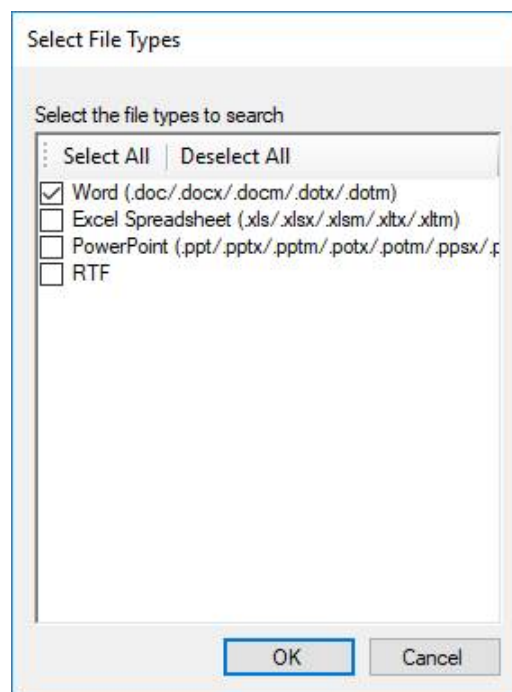
file type contains hidden data

This expression specifies that if Workshare Protect finds specified hidden data in a specified file type, then the condition will be met. Example: A Microsoft Excel document contains the track changes or version information.

File type

Clicking the **file type** expression link displays the *Select File Types* dialog.

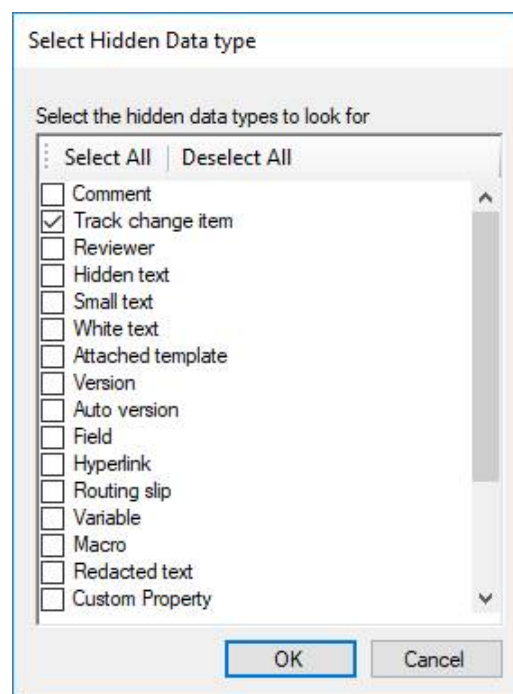
Select the file type(s) that you want the expression to cover and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file types.



Hidden data

Clicking the **hidden data** expression link displays the *Select Hidden Data type* dialog.

Select the hidden data types that you want to find in the document by clicking the corresponding checkboxes and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different hidden data types.



The different hidden data types are as follows:

- **Comment:** Cleans comments embedded in the document.
- **Track change item:** Cleans revisions made to the document.
- **Reviewer:** Cleans information about all document reviewers who have made changes in the document.
- **Hidden text:** Cleans text that has been formatted as hidden
- **Small text:** Cleans text that has been formatted with a font size less than 5 pt.
- **White text:** Cleans text that has been formatted with a font color of white and has no background color.
- **Attached template:** Cleans the template attached to a Microsoft Office document.
- **Version:** Cleans records of previous saved versions of the document.
- **Auto version:** Cleans records of previous auto-saved versions of the document
- **Field:** Cleans field codes that exist in a Microsoft Office document.
- **Hyperlink:** Cleans hyperlinks contained within a Microsoft Office document.
- **Routing slip:** Cleans entries from a routing slip, including the message subject and text.
- **Variable:** Cleans variable values stored in Microsoft Word documents that are used by either field codes or macros.
- **Macro:** Cleans VBA macros associated with a document.
- **Redacted text:** Cleans redacted (censored) text.
- **Custom Property:** Cleans property fields added manually to a document or added by various programs.
- **Built-in Property:** Cleans document summary properties, including author, category, comments, and other properties.
- **Document Statistic:** Cleans document statistics, including total edit time, revision number, and last saved by.
- **Footnote:** Cleans any footnotes or endnotes from Microsoft Word documents.
- **Smart tag:** Cleans smart tags from Microsoft Word documents.
- **Ink Annotations:** Cleans ink annotations made in Tablet PC.
- **Workshare Styles:** Cleans Workshare styles, which are the styles applied to the changes shown in a Redline document.

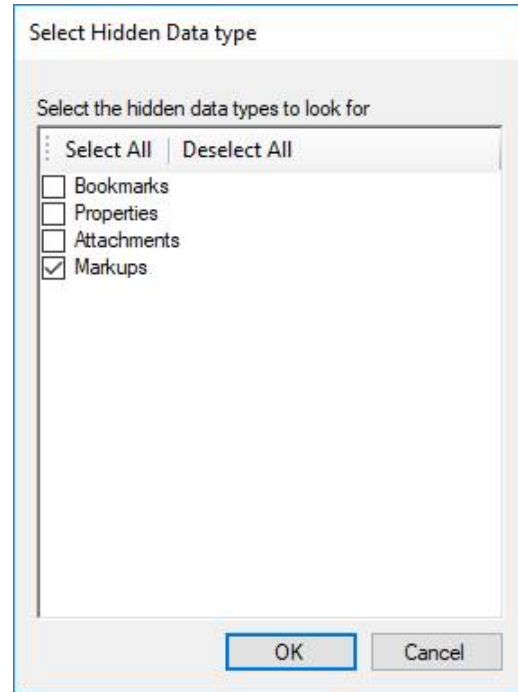
PDF file contains hidden data

This expression specifies that if Workshare Protect finds specified hidden data in a PDF file, then the condition will be met. Example: A PDF contains an attachment or markup.

Hidden data

Clicking the **hidden data** expression link displays the *Select Hidden Data type* dialog.

Select the hidden data types that you want to find in the PDF by clicking the corresponding checkboxes and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different hidden data types.



The different hidden data types are as follows:

- **Bookmarks:** Cleans any bookmarks from the PDF file.
- **Properties:** Cleans removes properties from the PDF file.
- **Attachments:** Cleans any attachments to the PDF file.
- **Markups:** Cleans any markup from the PDF file.

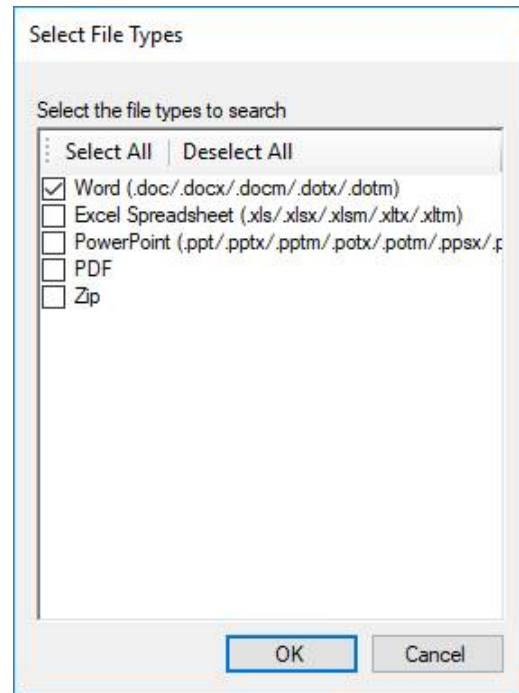
file type is password protected

This expression specifies that if Workshare Protect finds a specified file type is password protected, then the condition will be met. Example: A Microsoft Word document is password protected.

File type

Clicking the **file type** expression link displays the *Select File Types* dialog.

Select the file type(s) which if password protected will trigger the expression and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file types.



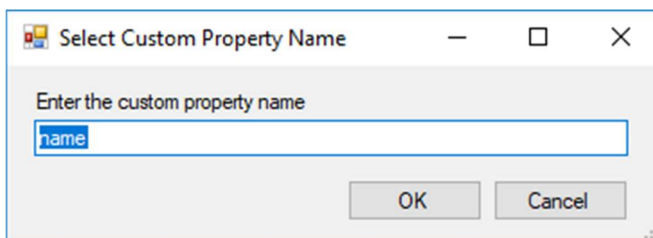
custom property name is value

This expression specifies that if Workshare Protect finds that a document contains a specified custom property with a specified value, then the condition will be met.

Example: A document contains the custom property “client” with the value “Workshare”.

Name

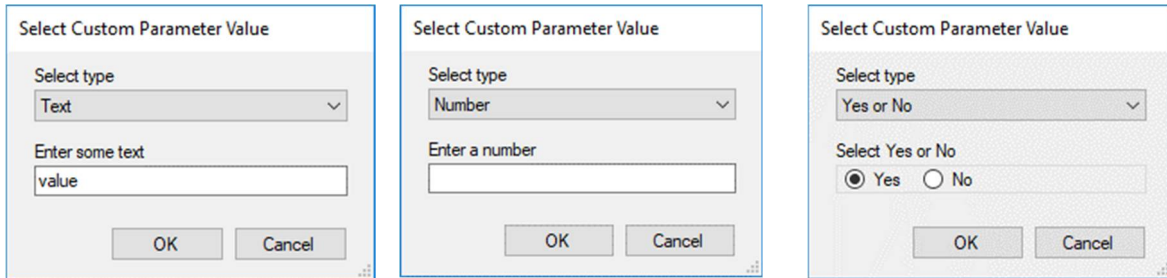
Clicking the name expression link displays the *Select Custom Property Name* dialog.



Enter the name of the custom property required to trigger the expression and click **OK**.

Value

Clicking the value expression link displays the *Select Custom Parameter Value* dialog.



Enter text or a number or select **Yes** or **No** as the custom property value required to trigger the expression and click **OK**.

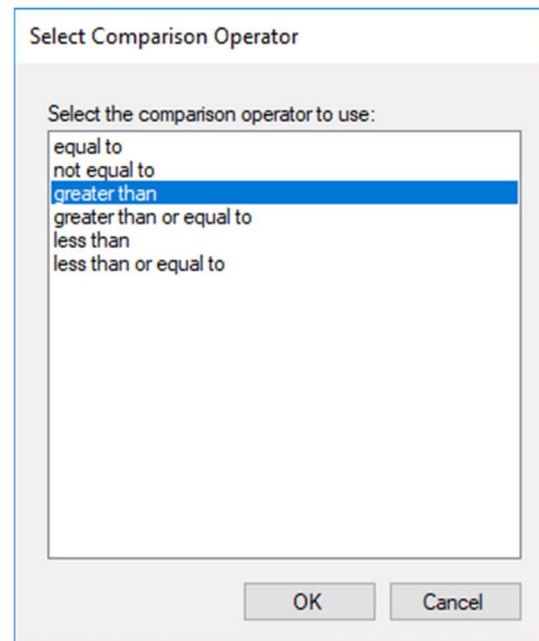
file size is compared against size Kb

This expression specifies that if Workshare Protect finds that a file has a specified relation (for example, greater than) to a specified size, the condition will be met. Example: A document is greater than or equal to 100 kb.

Compared against

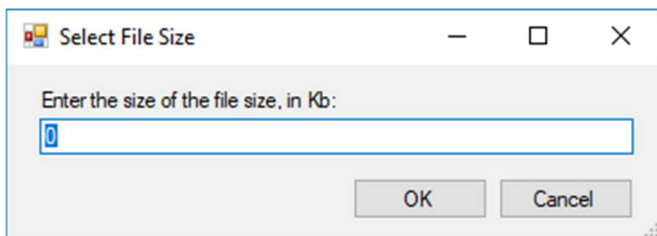
Clicking the **compared against** expression link displays the *Select Comparison Operator* dialog.

Select the comparison operator option against which you want the file size to be measured and click **OK**.



Size

Clicking the **size** expression link displays the *Select File Size* dialog.



Enter the file size required to trigger the expression and click **OK**.

file type is file type

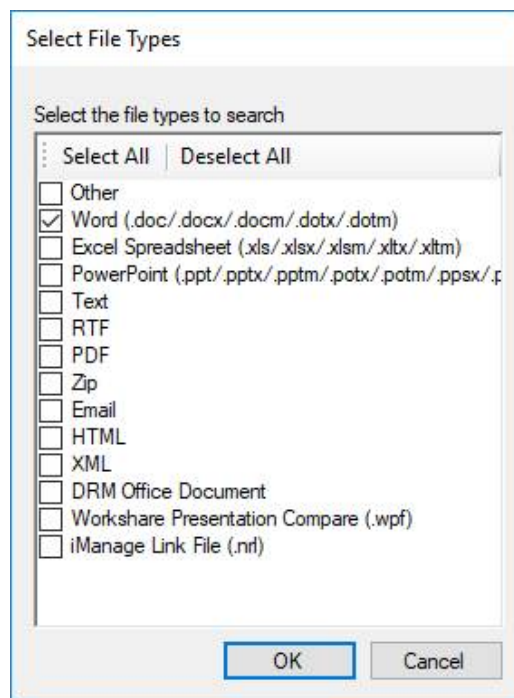
This expression specifies that if Workshare Protect finds that a file is of a specified type, then the condition will be met. Example: A file is a PowerPoint document”.

File type

Clicking the **file type** expression link displays the *Select File Types* dialog.

Select the file type(s) which will trigger the expression and click **OK**. You can use the **Select All** and **Deselect All** buttons to aid you in the selection of the different file types.

Note: An **.nrl** file is a link to a file located in *iManage*, which can only be accessed by recipients if they have access to the *iManage* server. Some users accidentally send these files externally instead of sending a copy of the actual document. You can use this expression to craft a custom policy to block these files from being sent to external users.



contains embedded email

This expression specifies that if Workshare Protect finds that a document contains an embedded email, then the condition will be met.

When working with Microsoft Outlook, Workshare analyzes embedded emails and their contents to see if they breach any policies. However, when working with IBM Lotus Notes, Workshare will not analyze embedded emails. In this scenario, if a policy includes this expression, then Workshare will detect an embedded email and show a policy breach.

Email has email address or domain within recipients address fields

This expression specifies that if Workshare Protect finds a specified email address or domain in any of the specified address fields, the condition will be met. Example: An email is being sent to or copied to (To or Cc) any email address in the workshare.com domain.

Email address or domain

Clicking the **email address or domain** expression link displays the *Specify email addresses or domains* dialog.

Enter the email address or domain name which will trigger the expression and click **Add**.

Click **OK**.

The dialog box titled "Specify email addresses or domains" contains a text input field labeled "Add the email address or domain" with an "Add" button to its right. Below this is a larger list box labeled "Look for the following email addresses or domains" with a "Remove" button to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

Recipients

Clicking the **recipients** expression link displays the *Select email address type* dialog.

Select the address fields where the specified email address or domain may be found in order to trigger the expression and click **OK**.

The dialog box titled "Select email address type" contains a section labeled "Look in the following address fields" with "Select All" and "Deselect All" buttons. Below this is a list of address fields with checkboxes: "From" (unchecked), "To" (checked), "Bcc" (checked), and "Cc" (checked). At the bottom of the dialog are "OK" and "Cancel" buttons.

Email has only email address or domain within recipients address fields

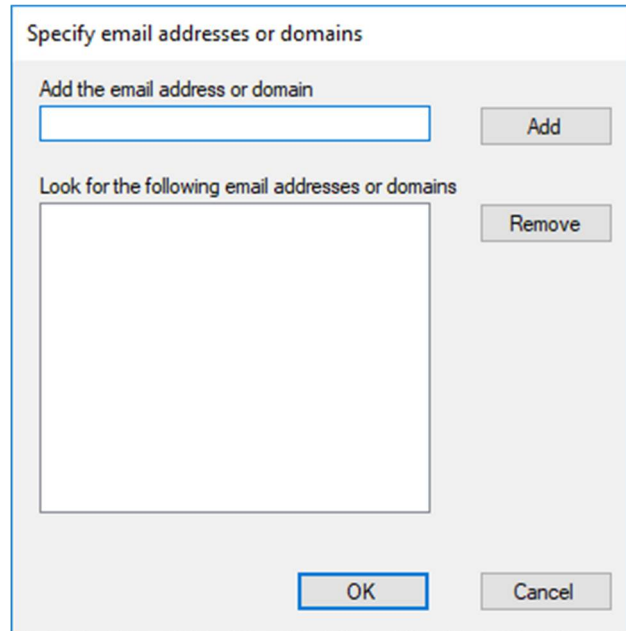
This expression specifies that if Workshare Protect finds **only** the specified email address or domain in any of the specified address fields, the condition will be met.

Email address or domain

Clicking the **email address or domain** expression link displays the *Specify email addresses or domains* dialog.

Enter the email address or domain name which will trigger the expression and click **Add**.

Click **OK**.

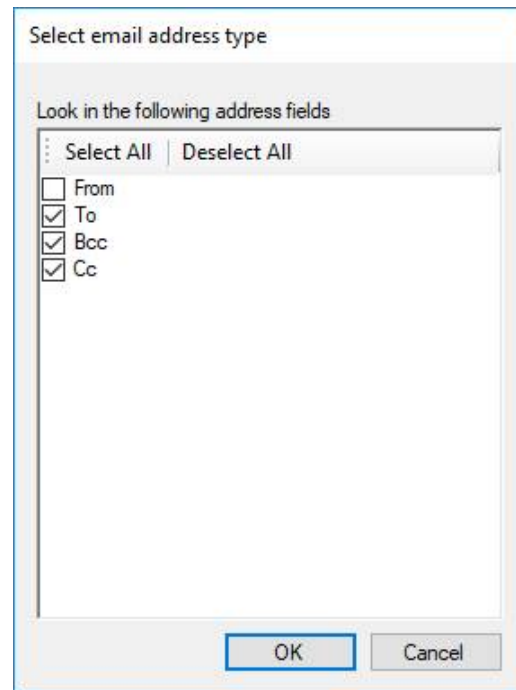


The dialog box titled "Specify email addresses or domains" contains a text input field labeled "Add the email address or domain" with an "Add" button to its right. Below this is a larger list box labeled "Look for the following email addresses or domains" with a "Remove" button to its right. At the bottom of the dialog are "OK" and "Cancel" buttons.

Recipients

Clicking the **recipients** expression link displays the *Select email address type* dialog.

Select the address fields where the specified email address or domain may be found in order to trigger the expression and click **OK**.



The dialog box titled "Select email address type" contains a section labeled "Look in the following address fields" with "Select All" and "Deselect All" buttons. Below this is a list of email address fields with checkboxes: "From" (unchecked), "To" (checked), "Bcc" (checked), and "Cc" (checked). At the bottom of the dialog are "OK" and "Cancel" buttons.

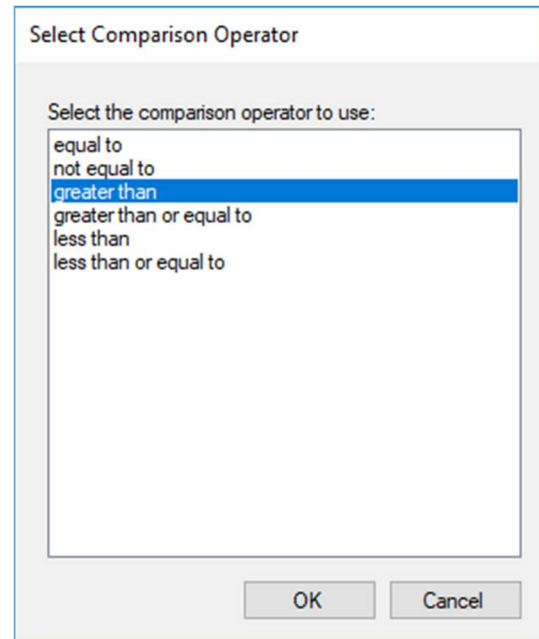
Total attachment size is compared against size Kb

This expression specifies that if Workshare Protect finds that the total size of all the attachments has a specified relation (for example, greater than) to a specified size, the condition will be met. Example: All the attachments are greater than or equal to 100 kb.

Compared against

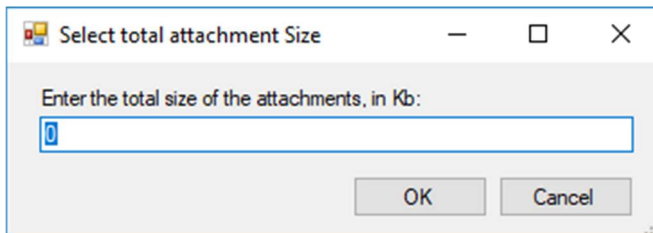
Clicking the **compared against** expression link displays the *Select Comparison Operator* dialog.

Select the comparison operator option against which you want the file size to be measured and click **OK**.



Size

Clicking the **size** expression link displays the *Select File Size* dialog.



Enter the file size required to trigger the expression and click **OK**.

Chapter 6: Channels and Action Sets

This chapter describes how to define action sets for different policy sets. It includes the following sections:

- [Introducing Channels and Action Sets, page 55](#)
- [Client Email Channel, page.55](#)
- [Active Content Channel, page 72](#)

Introducing Channels and Action Sets

An action set consists of one or more actions that are applied when a given condition is met. The actions available in the Policy Designer vary according to the channel selected. (Policy sets are defined based on channels.) A summary of the actions available is provided in the following table:

Channel	Data Monitored	Available Actions
Client Email	Emails and attachments sent by Microsoft Outlook and IBM Lotus Notes	<p>Block: The email is blocked and cannot be sent.</p> <p>Alert: The sender is alerted to the presence of suspicious content in the email and/or attachment but can still send the email.</p> <p>LightSpeed Clean: The suspicious content is removed from the attachment before it is sent.</p> <p>Clean: The suspicious content is removed from the attachment before it is sent.</p> <p>PDF: The attachment(s) is converted to PDF before the email is sent.</p> <p>PDFClean: The suspicious content is removed from PDF attachments before the email is sent.</p> <p>Zip: The attachment(s) is compressed into a zip file before the email is sent.</p> <p>Secure File Transfer: The attachment(s) is sent to a secure folder in Workshare online and recipients are sent a link to that location.</p>
Active Content	Open Microsoft Office documents	<p>Alert: The suspicious content is displayed in a content risk report.</p>

Client Email Channel

Policies defined for this channel are applied to emails and their attachments. When defining policies for the Client Email channel, you can specify the following actions for a policy breach:

- **Block:** The email is blocked and cannot be sent.
- **Alert:** The sender is alerted to the presence of suspicious content in the email and/or attachment but can still send the email.
- **LightSpeed Clean/Clean:** The suspicious content is removed from the attachment before it is sent.
- **PDF:** The attachment(s) is converted to PDF before the email is sent.
- **PDFClean:** The suspicious content is removed from PDF attachments before the email is sent.

- **Zip:** The attachment(s) is compressed into a zip file before the email is sent.
- **Secure File Transfer:** The attachment(s) is sent to a secure folder in Workshare online and recipients are sent a link to that location.

Note: If an action set includes multiple actions, there is an action precedence performed in the order of **Clean** or **Lightspeed Clean** or **PDF Clean**, **PDF**, **Zip**, and then **Secure File Transfer**.

Actions are specified according to senders and receivers. For example, where an email meets a condition (such as “includes the words private and confidential”), you can specify a **Block** action when the email is being sent from user group A to user group B and an **Alert** action when the email is being sent from user group A to user group C.

Information about sender and receiver groups is displayed in the routing table in the Workshare Policy Designer. The routing table enables you to distinguish between privileged and non-privileged senders of information and trusted and non-trusted receivers of information.

Routing for Client Email channel

Workshare Protect uses one of two routing types, as follows:

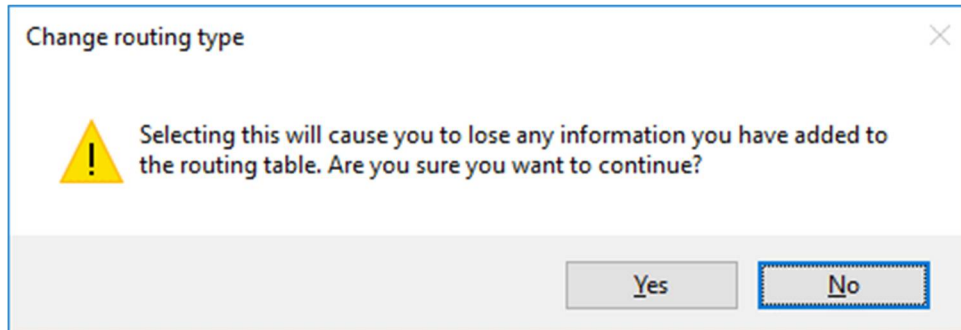
- **Default routing:** Workshare Protect simply distinguishes between internal and external users. For more information, refer to Default Routing on page 57.
- **Custom routing:** Workshare Protect distinguishes between all the different routing groups you have defined. For more information, refer to Custom Routing on page 57.

To select the routing type:

1. Open a Client Email policy set.
2. Expand the policy into which you want to specify routing in the Policy Set Explorer tree and select **Email Channel**. The *Channels, Routings and Actions* window is displayed in the right-hand pane of the Policy Designer window.

Tip: You can also click **Next** in the Condition window.

3. From the **Routing type** dropdown list above the routing table, select the routing type required: **Default routing** or **Custom routing**. When you change the routing type, the *Change routing type* message is displayed.



4. Click **Yes**.

Default routing

When you have selected Default routing as the routing type, you then select an action set for internal recipients and external recipients and Workshare Protect simply distinguishes between internal and external recipients when determining which action to apply. Thus, when you send an email, Workshare Protect takes each recipient in the **To**, **Cc** and **Bcc** fields, and looks them up in the local address book. For each address there are three possible outcomes:

- The address does not exist in the address book. This is then processed as external.
- The address is a distribution list. In this case, the address of each member of the distribution list is checked.
- The address exists in the address books. This is then processed as internal.

If the email is being sent to multiple recipients and an external recipient is found, then Workshare Protect applies the action specified for an external recipient even though some recipients may be internal. Only if all recipients are internal, is the action specified for an internal recipient applied.



Custom routing

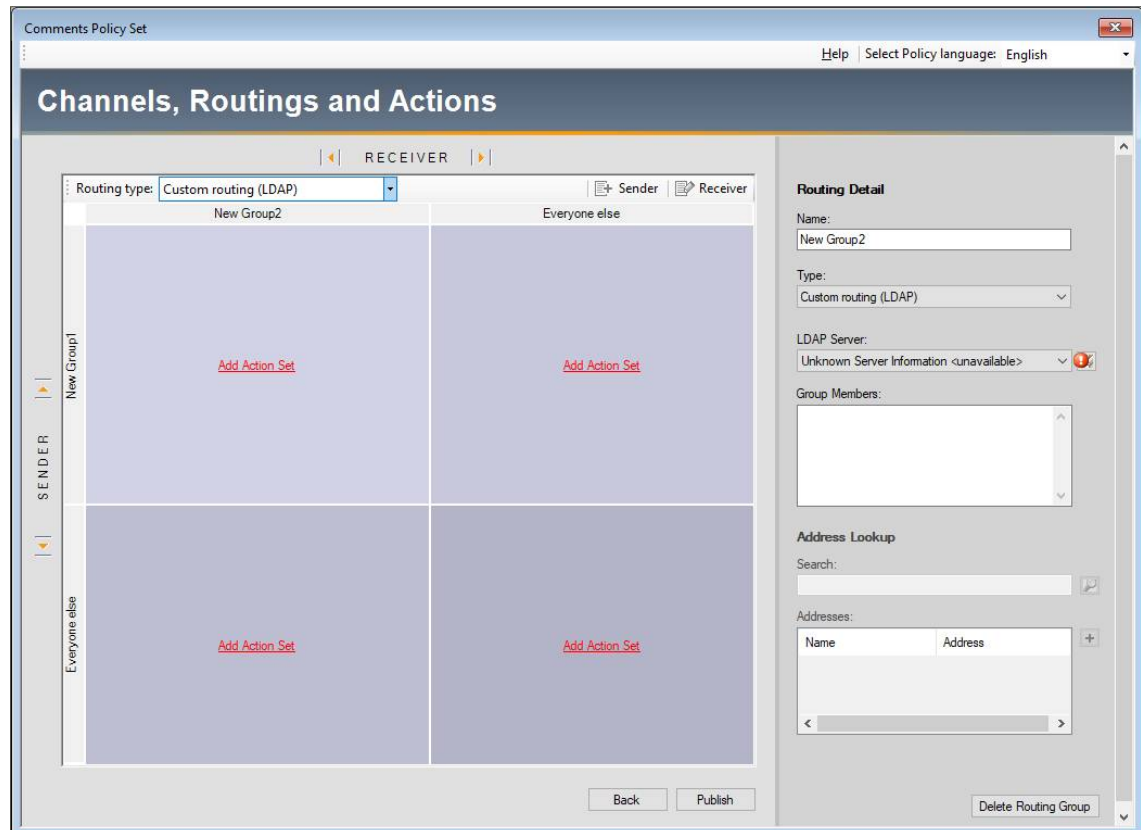
When you have selected Custom routing, you then define sender and receiver groups and select action sets for each combination, for example, when the email triggering the policy is from Sender Group A to Receiver Group B, then a Block action is applied. The Workshare Policy Designer routing table includes one receiver group (**Everyone else**) and one sender group (**Everyone else**). You add additional sender and receiver groups as required.



Adding new routing groups

The procedure for adding a new receiver group or a new sender group is the same.


To create a new routing group:

1. In the routing table, click the **Sender**  or **Receiver**  button. A new sender group **NewGroupX** is added to the **Sender** rows of the routing table or a new receiver group **NewGroupX** is added to the **Receiver** columns of the routing table and the *Routing Detail* dialog is displayed to the right of the routing table.



2. In the **Name** field, enter a relevant name for the routing group based on the members contained within (for example, “*Marketing*”). This name is displayed as the row or column header in the routing table.
3. In the **Search** field in the **Address Lookup** area, enter your search criteria and click the  button. The Workshare Policy Designer looks in the global address book and a list of addresses that match the search criteria are displayed in the **Addresses** list in the **Address Lookup** area. You can search for individual addresses or pre-defined distribution lists.
4. Select the relevant address or distribution list for this particular routing group in the **Addresses** list in the **Address Lookup** area and click the  button. The selected address or distribution list is added to the **Group Members** list.

Tip: Select multiple addresses or distribution lists by holding down the **Ctrl** or **Shift** key when selecting.

5. Click the  icon or select **Save** from the *File* menu. The new routing group is saved.

You can add additional routing groups to the routing table by repeating the procedure above or you can go on to specify actions for specific routing groups (see *Creating Action Sets for Client Email Channel*, page 63 for more information).

Viewing and editing existing routing groups

This section provides instructions for viewing and editing existing routing groups.

To view routing group members:

In the routing table, select the header of the sender or receiver group whose members you want to view. The *Routing Detail* dialog is displayed to the right of the routing table. The members of the selected group are listed in the **Group Members** list.

You can make changes to the selected routing group as follows:

- Change the name of the routing group by editing the **Name** field.
- Add additional users to the routing group using the procedure described in *Adding New Routing Groups*, page 58.
- Delete users from the routing group by selecting the user in the **Group Members** list and pressing the **Delete** key on your keyboard.

Note: You must save the open policy set before closing it to ensure that any changes that are made are saved.

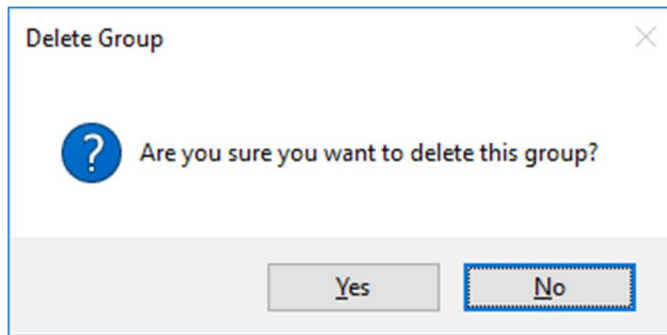
Deleting routing groups

This section provides instructions for deleting routing groups.

To delete a routing group:

1. In the routing table, select the header of the sender or receiver group that you want to delete. The *Routing Detail* dialog is displayed to the right of the routing table.

2. Click **Delete Routing Group** at the bottom of the *Routing Detail* dialog. The following prompt is displayed.



3. Click **Yes** to delete the routing group or click **No** to cancel.

The routing group is deleted from the routing table.

Note: You must save the open policy set before closing it to ensure that this routing group is permanently deleted from the policy set.

Understanding the routing table

The Workshare Policy Designer routing table defines actions according to sender and receiver groups using a system of precedence to rank these actions. The precedence increases from left to right. Thus, you should assign the least restrictive action in the top left-hand corner of the routing table (which is the square with the lightest tone) and the most restrictive action in the bottom right-hand corner of the routing table (which is the square with the darkest tone).

Example custom routing table

Channels, Routings and Actions

RECEIVER

Routing type: Custom routing (LDAP)

Sender

Receiver

	Management	Sales	IT	Everyone else
Marketing	Marketing - Management	Marketing - Sales	Marketing - IT	Marketing - Everyone else
Everyone else	Everyone else - Management	Everyone else - Sales	Everyone else - IT	Everyone else - Everyone else

Back

Publish

Example default routing table

The screenshot shows a web interface titled "Channels, Routings and Actions". At the top, there is a "RECEIVER" tab. Below it, a "Routing type" dropdown is set to "Default routing (internal / external)". The main area is divided into two columns: "Internal Recipients" and "External Recipients". On the left, a "SENDER" tab is visible, with "Everyone" selected. The "Internal Recipients" column contains a red text label "Everyone - Internal Recipients". The "External Recipients" column contains a red text label "Everyone - External Recipients". At the bottom right, there are "Back" and "Publish" buttons.

The following scenarios might arise:

- **Sending to Multiple Receiver Groups**

When information is sent to members of different receiver groups, the action that is executed is that of the most restricted group. Using the example custom routing table on page 61, if someone in Marketing sends an email to both Management and Sales, it is the action defined in the **Marketing-Sales** square of the table that is executed because Sales is the most restricted of the two groups. Using the example default routing table above, if someone in Marketing sends an email to an internal and external user, it is the action defined in the **Everyone-External Recipients** square of the table that is executed.





- **Sending to Users in Multiple Receiver Groups**

When a user is in more than one group, the action that is executed is that of their least restrictive group. Using the example routing table on page 61, if someone in Marketing sends an email to John (who is in both the Management and IT receiver groups), John's least restrictive group is Management and consequently it is the action defined in the **Marketing-Management** square of the table that is executed. However, if someone in Marketing sends an email to John (who is in both the Management and IT receiver groups) and Peter (who is in both the Sales and IT receiver groups), using the order of precedence described in *Sending to Multiple Receiver Groups*, it is the action defined in the **Marketing-IT** square of the table that is executed because the most restrictive group of John and Peter is IT.

- **Repositioning Senders and Receivers in the Routing Table**

When you have selected Custom routing, once you have created the routing table, you can change the order of the sender and receiver groups by repositioning them within the routing table.

To reposition a routing group, click the relevant sender or receiver group header in the table and select the appropriate button from the following:

- Click  to move a receiver group to the left.
- Click  to move a receiver group to the right.
- Click  to move a sender group up.
- Click  to move a sender group down.

Note: *If you are moving a routing group more than one place within the routing table, you have to repeat this process until they are in the correct position. However, you will not be able to move a routing group you have created beyond the default group of **Everyone else**.*

Creating action sets for Client Email channel

When defining policies that cover emails and their attachments, you can specify actions according to senders and receivers. If you do not specify particular sender or receiver groups, Workshare Protect applies the action defined for the default groups - sender **Everyone else** to recipient **Everyone else**.

An action set can include several actions. However, the following limits apply:

- After defining a Block action, you cannot add any further actions.
- After defining an Alert action, you can add a Clean, PDF or Zip action.
- After defining a LightSpeed Clean action, you can add an Alert, PDF or Zip action.
- After defining a PDF action, you can add an Alert, Clean or Zip action.
- After defining a Zip action, you can add an Alert, Clean or PDF action.
- It is not possible to add the same action within the same routing group.

- It is possible to add two of the above actions for two different routing groups and policies.
- If two different policies have been created with the same action then Workshare Protect will pick the first one it finds in the policy set.

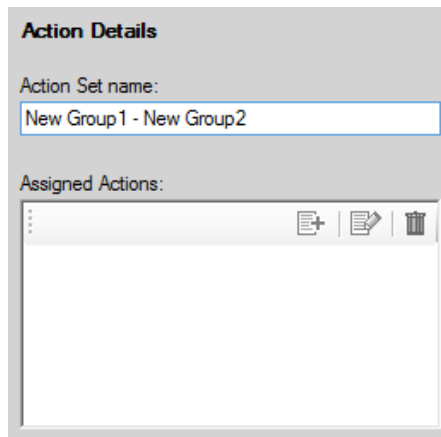
To create an action set for a Client Email channel:

1. Open a Client Email policy set.
2. Expand the policy into which you want to add the new action set in the Policy Set Explorer tree and select **Email Channel**. The *Channels, Routings and Actions* window is displayed in the right-hand pane of the Policy Designer window.
3. From the **Routing type** dropdown list (above the routing table) select **Custom routing** or **Default routing**. If you selected **Custom routing**, add the required routing groups to the routing table using the procedure described in *Add New Routing Groups*, page 58.

The screenshot displays the 'Channels, Routings and Actions' configuration window. At the top, there's a header bar with the title. Below it, a navigation pane on the left shows a tree structure with 'SENDER' and 'RECEIVER' sections. The main area is a routing table with two rows: 'New Group3' and 'Everyone else'. Each row has a large square area with a red 'Add Action Set' link. Above the table, there's a 'Routing type' dropdown set to 'Custom routing (LDAP)' and buttons for 'Sender' and 'Receiver'. To the right of the table is a 'Routing Detail' panel with fields for 'Name' (New Group3), 'Type' (Custom routing (LDAP)), 'LDAP Server' (Unknown Server Information <unavailable>), and 'Group Members'. Below this is an 'Address Lookup' panel with a 'Search' field and an 'Addresses' table with columns 'Name' and 'Address'. At the bottom of the window are 'Back', 'Publish', and 'Delete Routing Group' buttons.

4. In the routing table, click **Add Action Set** in the square relating to the recipient and sender to whom the action will apply. For example, in the sample routing table shown above, select **Add Action Set** in the top square if you want to define the action to be applied when an email from a user in **NewGroup1** group sends an email that triggers the condition defined in the selected policy.

The *Action Details* dialog is displayed to the right of the routing table.




Action Details

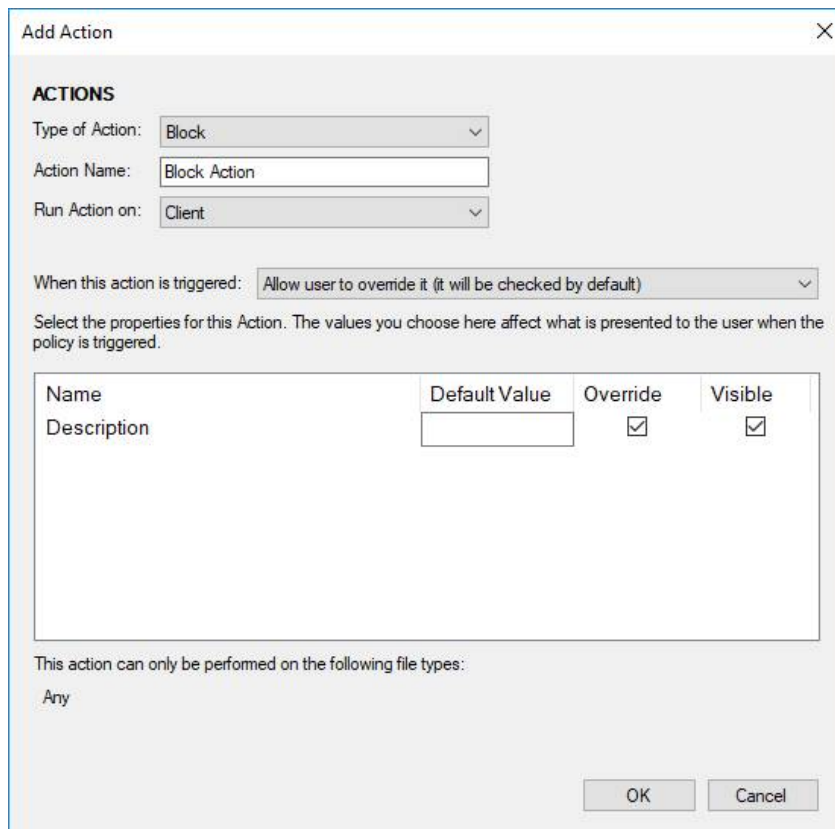
Action Set name:

Assigned Actions:

Icons: +, - (with document icon), trash

Note: The default name for the action set is the routing path of sender group to recipient group and this is displayed in the Action Set name field and in the routing table.

5. If required, modify the default name for the action set in the **Action Set name** field.
6. In the **Assigned Actions** list, click the **Add a new Action**  button. The *Add Action* dialog is displayed.



Add Action [X]

ACTIONS

Type of Action:

Action Name:

Run Action on:

When this action is triggered:

Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Description	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This action can only be performed on the following file types:

OK Cancel

7. From the **Type of Action** dropdown list, select one of the following actions that will be applied if the email or its attachment meets the defined condition:
 - **Block** – Blocks the email from being sent.
 - **Alert** – Alerts the user to a potential policy violation in the message or attachment.
 - **LightSpeed Clean** – Cleans metadata from Office attachments.
 - **Clean** – Cleans metadata from Office attachments.
 - **PDF** – Converts the attachment to PDF.
 - **PDFClean** – Cleans metadata from PDF attachments.
 - **Zip** – Compresses the attachment into a zip file.
 - **Secure File Transfer** – Sends the attachment to a secure folder in Workshare online and recipients are sent a link to that location.

Note: *Redact Clean, RPost Registered Email and PGP Universal Encryption relate to deprecated functionality and should be ignored.*

8. Enter a name for the action in the **Action Name** field based on its function within the policy (for example, “Clean Document Statistics and Built in Properties”). This name is displayed in the **Assigned Actions** list.
9. From the **When this action is triggered** dropdown list, select one of the following options that will determine if the action can be overridden by users when a policy is triggered:
 - **Always execute (the user will be unable to uncheck it)**
 - **Allow user to override it (it will be checked by default)**
 - **Allow user to override it (it will be unchecked by default)**

The dialog varies according to the type of action selected in Step 7.

10. When selecting a **Block** or **Alert** action, enter a relevant description in the **Default Value** field. This description is displayed in the Workshare Protect *Email Security* dialog to provide an explanation for the user.

11. When selecting a **Clean** or **LightSpeed Clean** action, select the checkboxes boxes in the **Default Value** column next to the cleaning options you want to be applied by default.

Add Action [X]

ACTIONS

Type of Action: Clean [v]

Action Name: Clean Action

Run Action on: Client [v]

☐ Process Transparently

When this action is triggered: Allow user to override it (it will be checked by default) [v]

Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Footnotes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Document Statistics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Built In Properties	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Headers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Footers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Smart Tags	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Template	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Custom Properties	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This action can only be performed on the following file types:

.doc	.xls	.ppt	.docx	.docm	.dotx	.dotm
.xlsx	.xlsm	.xltx	.xltm	.pptx	.pptm	.potx
.potm	.ppsx	.ppsm	.rtf			

OK Cancel

Note: For detailed information about the data that can be cleaned using the *LightSpeed Clean* action, refer to *Appendix C: Clean/LightSpeed Clean Action Properties*.

12. For the **PDF** action, select one or more of the security options by selecting the checkbox in the corresponding **Default Value** field.

ADD ACTION

ACTIONS

Type of Action: PDF

Action Name: PDF Action

Run Action on: Client

☐ Process Transparently

When this action is triggered: Allow user to override it (it will be checked by default)

Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Prohibit printing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prohibit modification of text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prohibit text or graphics being copied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prohibit comments being added	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password Required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enforce Strong Password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
REQUIRES APPROVAL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This action can only be performed on the following file types:

.doc	.xls	.ppt	.docx	.docm	.dotx	.dotm
.xlsx	.xlsm	.xltx	.xltm	.pptx	.pptm	.potx
.potm	.ppsx	.ppsm	.rtf			

OK Cancel

The options are as follows:

- **Prohibit Printing:** Prevents recipients from printing the PDF document.
- **Prohibit modification of text:** Prevents recipients with Adobe Distiller from editing the PDF document.
- **Prohibit text or graphics being copied:** Prevents recipients from copying graphics or text directly from the PDF document.
- **Prohibit comments being added:** Prevents recipients with Adobe Distiller from adding comments to the PDF document.
- **Password Required:** Requires a password to be set for the PDF.

- **Enforce Strong Password:** Requires a strong password to be set for the PDF. A strong password must be at least 8 characters long and contain at least one lower case letter, one upper case letter, one number, and one of the following special characters:
-+*\$%[]^().)|#|!@%&_=:;',/.
- **Password:** Type the password that is required for the PDF.
- **Apply to All:** Applies these settings to all documents.
- **Reconstruct Hyperlinks:** Preserves standard URL and bookmark hyperlinks.
- **PDF/A:** Sets the PDF/A option as the default when converting to PDF.

Note: Selecting the **Reconstruct Hyperlinks** option can increase the time it takes to create a PDF document. Hyperlinks that are preserved using this option may not correspond exactly to the location in the original document.

13. When selecting a **PDFClean** action, select the checkboxes boxes in the **Default Value** column next to the cleaning options you want to be applied by default.

Add Action ✕

ACTIONS

Type of Action: PDFClean ▾

Action Name: PDFClean Action

Run Action on: Client ▾

☐ Process Transparently

When this action is triggered: Allow user to override it (it will be checked by default) ▾

Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Bookmarks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Properties	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Attachments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Markups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apply to All	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This action can only be performed on the following file types:

.pdf

OK Cancel

The options are as follows:

- **Bookmarks:** Cleans any bookmarks from a PDF file.
- **Properties:** Cleans removes properties from a PDF file.
- **Attachments:** Cleans any attachments to a PDF file.
- **Markups:** Cleans any markup from a PDF file.
- **Apply to All:** Applies these settings to all documents.

14. For the **Zip** action, select one or more of the zip options by selecting the checkbox in the corresponding **Default Value** field.

Add Action [X]

ACTIONS

Type of Action: **Zip** ▼

Action Name: **Zip Action**

Run Action on: **Client** ▼

☐ Process Transparently

When this action is triggered: **Allow user to override it (it will be checked by default)** ▼

Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Password Required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enforce Strong Password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password	<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ZIP Attached Files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AES128	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply to All	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This action can only be performed on the following file types:

Any

OK Cancel

The options are as follows:

- **Password Required:** Requires a password to open the zip archive.
- **Enforce Strong Password:** Requires the use of a strong password.

Note: A “strong” password must be at least 8 characters long and contain at least one lower case alpha, at least one upper case alpha, at least one numeric and at least one of the following: - +*\$[]^().|#!@%&_=:;,./.

- **Password:** Type the password that is required to open the zip archive.
 - **Zip Attached Files:** Groups related files in a single zip archive.
 - **AES 128:** Applies AES 128-encryption to zip archives.
 - **Apply to All:** Applies these settings to all documents.
15. When selecting a **Clean**, **Lightspeed Clean**, **PDF**, **PDFClean** or **Zip** action, select the checkbox in the **Default Value** field for the **Apply To All** option if you want the **Apply To All** checkbox in the Workshare Protect *Email Security* dialog to be selected by default. This checkbox means that the specified clean, PDF or zip settings are applied to all attachments.
16. To enable the user to override any options within the action, select the checkbox in the corresponding **Override** field.
17. To enable the user to see the action options, select the checkbox in the corresponding **Visible** field. If you do not want to enable the user to see the action options, ensure the checkbox in the corresponding **Visible** field is deselected.
18. If you do not want the user to view any options within the action, select the **Process Transparently** checkbox. This means that the action is performed without displaying a dialog and the user cannot change the parameters of the action. The dialog will still be displayed if another “visible” policy is also triggered or if Workshare needs to prompt for a password.

Note: The **Process Transparently** checkbox is available in the Add Action dialog when **Clean**, **Lightspeed Clean**, **PDF**, **PDFClean** or **Zip** actions are selected. The checkbox may also be available when an **Alert** action is selected if it has been configured that way in the Actions Add-In Manager (described in Appendix D: Actions Add-In Manager).

19. Once all the relevant options have been selected, click **OK**. The new action is added to the selected routing choice and the name of the action set in the routing table changes to blue.
20. Optionally repeat steps 6 to 18 to add further actions to the action set.

Note: If you have added a **Block** action, you will not be able to add an additional action to the same action set. If you have added a **PDF** or **Zip** action, you are not able to add another **PDF** or **Zip** action to the same action set.

21. Click the  icon or select **Save** from the *File* menu. The new action set is saved.

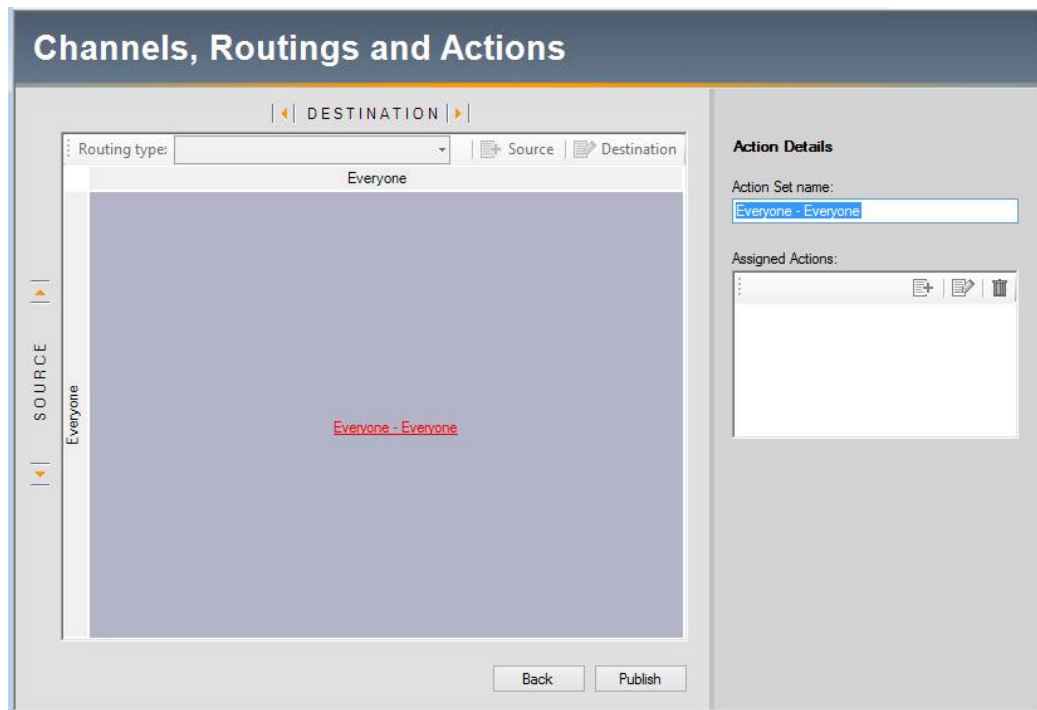
If all the elements of this policy have been completed, you can publish the policy by clicking **Publish**. For more information, refer to *Publishing Policy Sets*, page 76.

Active Content Channel

Policies defined for this channel are applied to open Microsoft Office documents. When defining policies for the Active Content channel, you specify an Alert action for a policy breach. In effect, active content policies determine what is displayed in the content risk report when a user clicks Content Risk in an open Office document.


To create an action set for an Active Content channel:

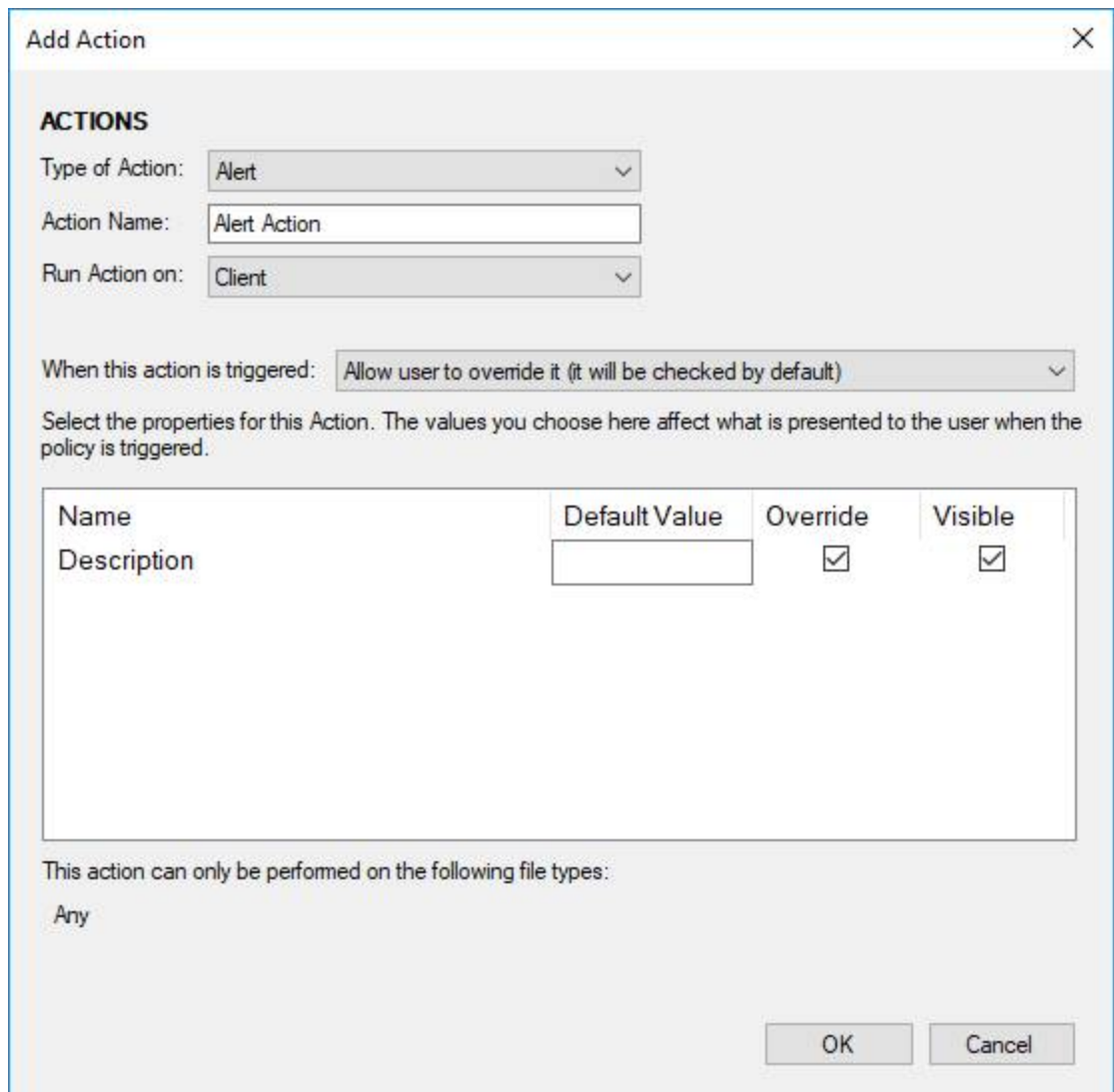
1. Open an Active Content policy set.
2. Expand the policy into which you want to add the new action set in the Policy Set Explorer tree and select **Active Content Channel**. The *Channels, Routings and Actions* window is displayed in the right-hand pane of the Policy Designer window.
3. In the routing table, click **Add Action Set**. The *Action Details* dialog is displayed to the right of the routing table.



Note: The default name for the action set is **Everyone-Everyone** and this is displayed in the **Action Set name** field and in the routing table.

4. If required, modify the default name for the action set in the **Action Set name** field.

5. In the **Assigned Actions** list, click the **Add a new Action**  button. The *Add Action* dialog is displayed.




The **Add Action** dialog box contains the following fields and options:

- ACTIONS**
 - Type of Action: Alert (dropdown)
 - Action Name: Alert Action (text field)
 - Run Action on: Client (dropdown)
- When this action is triggered: Allow user to override it (it will be checked by default) (dropdown)
- Select the properties for this Action. The values you choose here affect what is presented to the user when the policy is triggered.

Name	Default Value	Override	Visible
Description		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- This action can only be performed on the following file types:
 - Any
- Buttons: OK, Cancel

There is only one action type available from the **Type of Action** dropdown list- **Alert**.

6. Enter a name for the action in the **Action Name** field based on its function within the policy. This name is displayed in the **Assigned Actions** list.
7. From the **When this action is triggered** dropdown list, select one of the following options that will determine if the action can be overridden by users when a policy is triggered:
- **Always execute (the user will be unable to uncheck it)**
 - **Allow user to override it (it will be checked by default)**
 - **Allow user to override it (it will be unchecked by default)**

8. Enter a description for the action in the **Default Value** field.
9. To enable the user to override the description, select the checkbox in the **Override** field.
10. To enable the user to see the description, select the checkbox in the **Visible** field. If you do not want to enable the user to see the description, ensure the checkbox in the **Visible** field is deselected.
11. Click **OK**. The new action is added and the name of the action set in the routing table changes to blue.
12. Click the  icon or select **Save** from the *File* menu. The new action set is saved.

If all the elements of this policy have been completed, you can publish the policy by clicking **Publish**. For more information, refer to *Publishing Policy Sets*, page 76.

Chapter 7: Policy Activation

This chapter describes how to activate a policy and publish it on a standalone computer once all the elements have been completed. It includes the following section:

- Publishing Policy Sets, page 76

Publishing Policy Sets

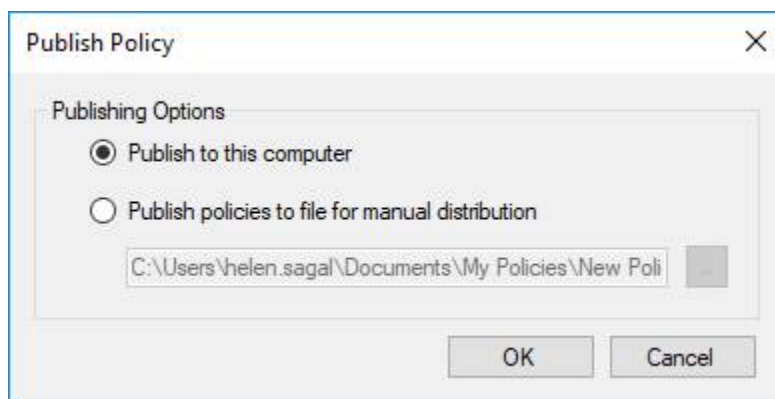
Once you are satisfied with all the elements of a particular policy set, you can activate the policy set by publishing it. You can publish policy sets to the local computer, which means the policies defined in the policy set will be applied when sending email or working on documents on the local machine. Alternatively, you can publish the policy set to a file for testing or for distribution to all machines on your network with Workshare Protect.

Note: When a policy set is published to the local computer, the `.runtimepolicy` file is saved in the `C:\Users>[user name]>AppData>Roaming>Workshare>PolicySets` directory and will only be applied to that user. For a locally published `.runtimepolicy` file to be applied to all users on the computer it must exist in the `C:\ProgramData\Workshare\PolicySets\ClientProfiles\Default` directory.

It is recommended that the `.runtimepolicy` files are deployed to the all users location through Active Directory group policy.

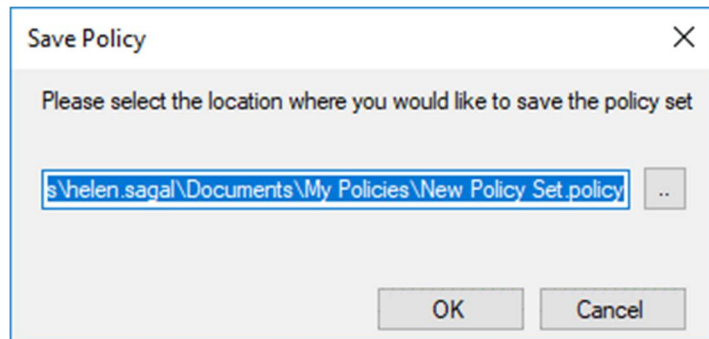
To publish a policy set:

1. Open the policy set that you want to publish.
2. Select **Publish** from the *File* menu or click **Publish** on the *Channels, Routing and Actions* window. The *Publish Policy* dialog is displayed.



3. Select one of the following options:
 - **Publish to this computer:** If you are using a standalone computer.
 - **Publish policies to file for manual distribution:** If you want to test the policy or if you want to deploy using a push method (for example, SMS). Click the Browse button to specify the `.runtimepolicy` file name and save location.
4. Click **OK**.

5. If you have not saved the policy set as a .policy file, you will be prompted to do so.



By default, .policy files are saved in **Modules>Sample Policies** in the install location.

6. Specify a name and location for the .policy file. This is the file you open in the Policy Designer if you want to edit this policy set further.
7. Click **OK**.

The policy set is saved as a .policy file and published as a .runtimepolicy file. Its status is **Enabled** in the Policy Set Explorer tree indicating that the policy set is now published.



Depending on the type of publication that you selected, the policy set is now activated on your local computer or saved ready for distribution.

Note: You can test the policies that you created by sending emails containing your specified triggers.

Chapter 8: Language Files

This chapter describes how to create new language versions of an existing policy set by exporting and importing language files. It includes the following sections:

- Overview of Language Files, page 79
- Exporting a Language File from a Policy Set, page 79
- Importing a Language File into a Policy Set, page 80

Overview of Language Files

In order to view an existing policy set in another language, you must perform the following steps:

1. Export the policy set as a TXT file and save it to a location.
2. Open the TXT file and translate as required.
3. Import the translated TXT file back into the Workshare Policy Designer.

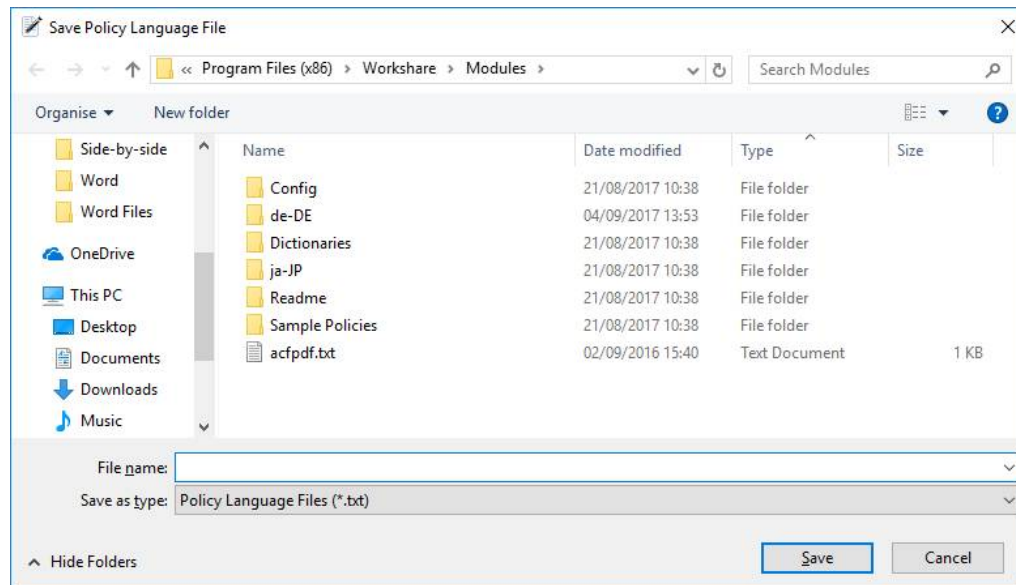
These steps are described in the following sections.

Exporting a Language File from a Policy Set

In the Workshare Policy Designer, you can export a language file from an existing policy set and save it to a location from where it can be translated into another language and then imported back into the policy set.

To export a language file:

1. Open the policy set that you want to translate into another language.
2. From the *File* menu, select **Language Resource File** and then **Save File**. The *Save Policy Language File* dialog is displayed.



3. Navigate to the required save location, enter a name for the policy set and click **Save**.

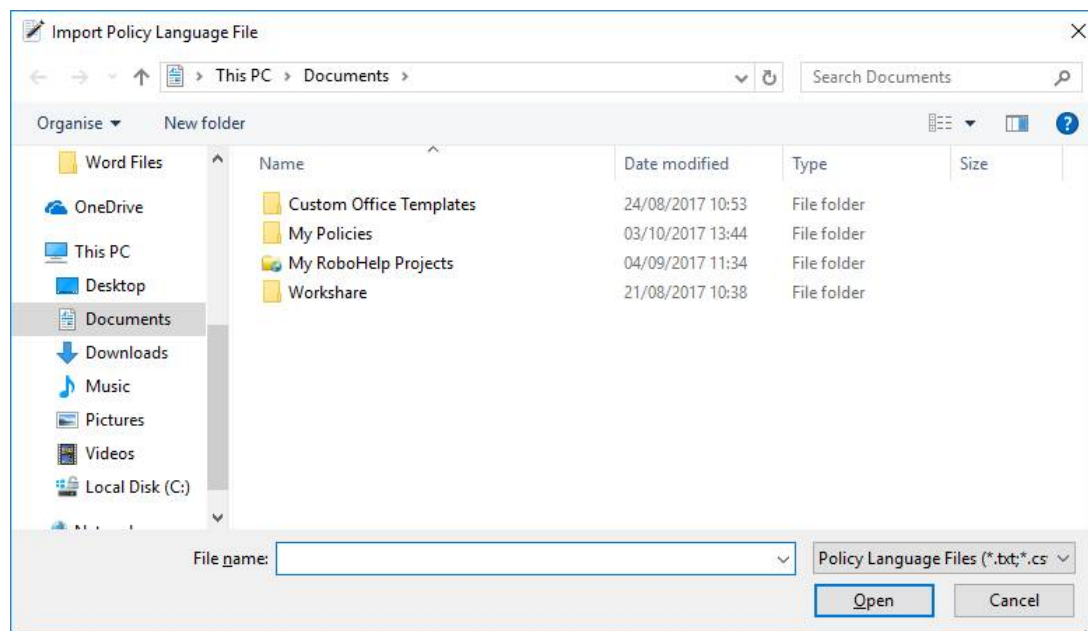
The selected policy set is saved as a TXT file. You can now open the saved TXT file (in Notepad or similar editor) and edit the contents into the required language. Once you have made the changes, save the TXT file and import it back into the same policy set.

Importing a Language File into a Policy Set

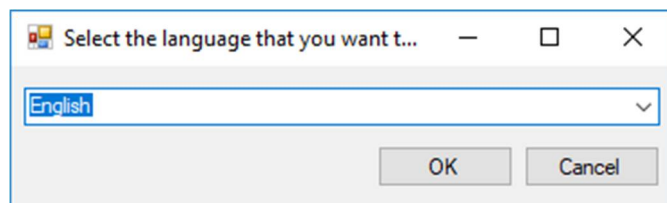
In the Workshare Policy Designer, you can export a language file from an existing policy set, save it to a location where it can be translated into another language, and then import it back into the policy set.

To import a language file:

1. Open the policy set from which you exported the language file.
2. From the **File** menu, select **Language Resource File** and then **Load File**. The *Import Policy Language File* dialog is displayed.



3. Navigate to the location where the TXT file is saved, select the CSV file and click **Open**. The *Select the language that you want to import* dialog is displayed.



4. Select the language of the translated TXT file from the dropdown list and click **OK**.

The selected language file is imported into the policy set. You can now select the different language versions of the policy set from the **Select policy Language** dropdown list.

Note: You must save the open policy set before closing it to ensure that any changes that are made are saved. You will also have to republish the policy set to activate both language versions

Appendix A.Regular Expressions

This appendix provides information on all the different types of regular expressions available in the Workshare Policy Designer.

Introducing Regular Expressions

A regular expression is an expression that describes a set of strings according to certain syntax rules. They are usually used to give a concise description of a set, without having to list all elements. While regular expressions may appear complex, they can be easily modified to suit your needs. Several tools exist to help you create new regular expressions and validate them as well. At the end of the chapter is a list available tools that to help you further understand how you can customize your existing conditions.

Here are some guidelines to help you create new regular expressions or customize existing ones:

- Use regular expressions syntax based on .NET.
- Use existing regular expressions if possible. There are libraries of them available on the internet. You can start with <http://www.regexlib.com/>
- Test your new regular expression thoroughly. Again there are a number of tools available to help you ensure your regular expression will work with Workshare Protect. Be wary of false positives!

Regular Expression Applications

The following is a list of useful regular expression applications.

- www.regexbuddy.com/ : Complete tool for learning, creating, testing and saving regular expressions, with two way conversion between regex syntax and plain English building blocks, and a debugger that lets you see inside the regex engine. Windows and Linux versions are available.
- www.powergrep.com/ : Feature-rich Windows application to search, search and replace and collect data using one or more regular expressions.

Useful references

Regular expression tutorials and primers:

- <http://www.regular-expressions.info/tutorial.html> (for beginners)
- <http://msdn.microsoft.com/en-us/library/az24scfc.aspx> (for experienced regex users)
- <http://en.wikipedia.org/wiki/Regex>
- http://www.foo.be/docs/tpj/issues/vol1_2/tpj0102-0006.html
- <http://perl.plover.com/Regex/article.html>

Appendix B. Clean/LightSpeed Clean Action Properties

This appendix provides information about the different options available when configuring a **Clean** action or a **LightSpeed Clean** (binary cleaning) action for a Client Email channel. Refer to *Chapter 6: Channels and Action Sets* for more information on creating action sets.

Clean/LightSpeed Clean Action Options

This section provides a description of the items that can be cleaned from an email or attachment using the **Clean/LightSpeed Clean** action.

Parameter	Description
Footnotes	Microsoft Word only. Removes any footnotes or endnotes included in the document.
Document Statistics	Microsoft Word only. Resets all the document statistics - total edit time, revision number, last authors, and file dates.
Built-In Properties	Microsoft Word, Excel and PowerPoint. Removes all summary properties - author, category, comments, company, keywords, manager, title, subject, and hyperlink base; and custom properties – text, date and number.
Headers	Microsoft Excel and PowerPoint. Removes any headers included in the sheet or slide.
Footers	Microsoft Excel and PowerPoint. Removes any footers included in the sheet or slide.
Smart Tags	<p>Microsoft Word 2003/2007 only. Removes smart tags from Microsoft Word documents.</p> <p>Smart tags are added to your documents as you create them if the option is enabled. These tags are linked to particular text in a document, such as a name, and allow you to perform certain actions by selecting the link associated with the text. Depending on the smart tag functions you use, they may embed extra hidden information in your document.</p> <p>Smart tags only exist in Microsoft Office XP to 2010.</p>
Template	Microsoft Word only. Converts the attached template to normal.dot. 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.
Custom Properties	Microsoft Word, Excel and PowerPoint. Removes any custom properties that have been added to the document.
Document Variables	<p>Microsoft Word only. Deletes all document variables.</p> <p>Document variables are values stored in Microsoft Word documents that are used by either field codes or macros. These variables may contain confidential information like company names or file locations. Even if field codes and macros are removed, the variables used may remain in the document.</p> <p>Variables can be viewed in Microsoft Word in the Visual Basic Editor.</p>

Parameter	Description
Fields	<p>Microsoft Word, Excel and PowerPoint. Converts any field codes that exist in a Microsoft Word document to text, for example, hyperlinks, table of contents, index. In Microsoft Excel and PowerPoint, hyperlinks are converted to text.</p> <p>This prevents the field codes from being updated after you have distributed the document. It also prevents errors for fields that reference built-in or custom properties that have been removed.</p>
Macros	<p>Microsoft Word and Excel. Removes VBA macros from a document. This feature is not intended as virus protection, but rather to protect any confidential information, intellectual property or formulas included in the macros.</p>
Routing Slip	<p>Microsoft Word and Excel. Removes all entries from a routing slip, as well as the message subject and text. This can prevent email addresses of colleagues from being unknowingly distributed. This also deletes any envelope information, such as recipients, subject, and introduction, which are used when sending to a mail recipient.</p>
Speaker Notes	<p>Microsoft PowerPoint only. Deletes all text that appears on the Notes Page in a Microsoft PowerPoint presentation. This is usually used by speakers to remind them of points during a presentation. You may want to remove speaker notes before distributing a presentation, as they are not usually intended for others to read.</p>
Links	<p>Microsoft Excel only. Converts external links in Microsoft Excel files to text. The following are examples of external links:</p> <ul style="list-style-type: none"> • Link to a cell in another Microsoft Excel document. • Named link to a named reference in another Microsoft Excel document. • Link to another document. • OLE link that inserts another document as an icon. • OLE link that inserts another document as text.
Reviewers	<p>Microsoft Word only. Removes information about all document reviewers who have made changes in the document. Track changes are not removed, but information about the user who made the change is removed.</p>
Track Changes	<p>Microsoft Word and Excel. Accepts all revisions made to the document. The revisions are therefore no longer displayed as revisions but rather as text in the document. Track changes is also turned off so that further revisions are not tracked.</p>
Comments	<p>Microsoft Word, Excel and PowerPoint. Removes any comments embedded in the document.</p>

Parameter	Description
Small Text	Microsoft Word only. Removes all text that has been formatted with a font size less than 5pt (i.e. 4pt and less). Small text can also be detected in Microsoft Excel but it is not cleaned.
White Text	Microsoft Word only. Removes all text with a white font that has been formatted with a white background color.
Hidden Text	Microsoft Word only. Removes all text that has been formatted as hidden.
Authors	Microsoft Word only. Removes information about all authors who have previously saved the document as well as save locations. This information cannot be viewed from within Microsoft Word but it is visible from Microsoft Word if the file is opened in recovered text mode.
Hidden Slides	Microsoft PowerPoint only. Removes hidden slides from Microsoft PowerPoint files. Hidden slides are not required for a slide show (they are not automatically displayed during a slide show) but they may contain confidential information.
Auto Version	Microsoft Word only. Turns off the flag to automatically save a new version of the document every time the document is closed. This applies to local file systems only. Versions can still be saved manually by saving a file with a different name.
Versions	Microsoft Word only. Removes any previous versions of the document that you may have saved. Previous versions can be useful while you are developing a document, but often they can contain confidential information that you have removed from the main document.
Apply to All	Apply the selected settings to all documents.
Exclude Custom Properties	If you have custom properties in your documents that you never want to remove, for example, DMS DocIds, you can exclude them from both cleaning and discovery. To exclude custom properties, add the names of the custom properties to this parameter. If you want to specify more than one property you can do so by using a semicolon. For example, DocId;Department .
Exclude Field Codes with Author Information	These are field codes that include the Author, Last Saved By User, or Current User information. If selected, any field codes referencing the author or user are not cleaned.

Parameter	Description
Exclude Field Codes with Document Information	<p>These are field codes that reference any of the document properties, for example, subject and keywords, as well as any field codes that reference the document statistics, for example, create date and number of words.</p> <p>If selected, any field codes referencing the document properties or statistics are not cleaned.</p>
Exclude Field Codes for Form Fields	<p>These are field codes that are used in forms, for example, dropdown lists and text boxes.</p> <p>If selected, any form field codes are not cleaned.</p>
Exclude Field Codes for Include Fields	<p>These are field codes that include text or pictures from other sources.</p> <p>If selected, any 'include' field codes are not cleaned.</p>
Exclude Field Codes for Index and Tables	<p>These are field codes related to the Table of Contents, Table of Authorities, Glossary, and Index.</p> <p>If not selected, these tables are unlinked, and can therefore no longer be automatically updated.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>Note: <i>Unlinking a Table of Contents causes the hyperlinks that reference each section of the document to stop working. It may also change the format of the Table of Contents to blue underlined text.</i></p> </div>
Exclude Field Codes for Numbering	<p>These are field codes for numbering within the document, for example, page numbers, list numbers, section numbers.</p> <p>If not selected, these numbers are unlinked and therefore no longer automatically updated.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p>Note: <i>Unlinking page numbers in headers or footers may cause page numbers to be repeated if a header or footer is shared between more than one page of the document.</i></p> </div>
Exclude Field Codes for Hyperlinks	<p>These are field codes for hyperlinks.</p> <p>If not selected, hyperlinks are unlinked. The text of the link is still visible but the associated address is removed.</p>
Exclude Field Codes for Links	<p>These are field codes for linked or imported objects.</p> <p>If selected, the links are not removed and therefore still update from the source.</p>

Parameter	Description
Exclude Field Codes for References	These are field codes for any references within the document, for example, page references. If not selected, references are unlinked and therefore no longer automatically updated.
Exclude Field Codes for Equations and Formulas	These are field codes for calculations, for example, equations, symbols or formula. If selected, equations remain linked.
Exclude Field Codes for Document Automation	These are field codes used to provide functions within a document, for example, macro buttons, mail merge functions, print functionality. If selected, these field codes remain linked which means the document automation features continue to work.
Exclude Document Variables	If you have document variables in your documents that you never want to remove, you can exclude them from both cleaning and discovery. To exclude document variables, add the names of the document variable to this parameter. If you want to specify more than one document variable you can do so by using a semicolon.
Exclude Field Codes	If you have field codes in your documents that you never want to remove, you can exclude them from both cleaning and discovery. To exclude specific field codes, add the name of the field code to this parameter. If you want to specify more than one field code you can do so by separating each field code with a semicolon.
Delete Field Codes	Workshare Protect is configured to replace field codes with static text. However, by entering the field codes in this parameter, Workshare Protect will delete any instances of these field codes. To delete specific field codes, add the name of the field code to this parameter. If you want to specify more than one field code you can do so by separating each field code with a semicolon.
Handle Footnotes as hidden data	If selected, footnotes are also treated as hidden data.

Appendix C. Actions Add-In Manager

This appendix describes the functionality of the Actions Add-In Manager. It includes the following sections:

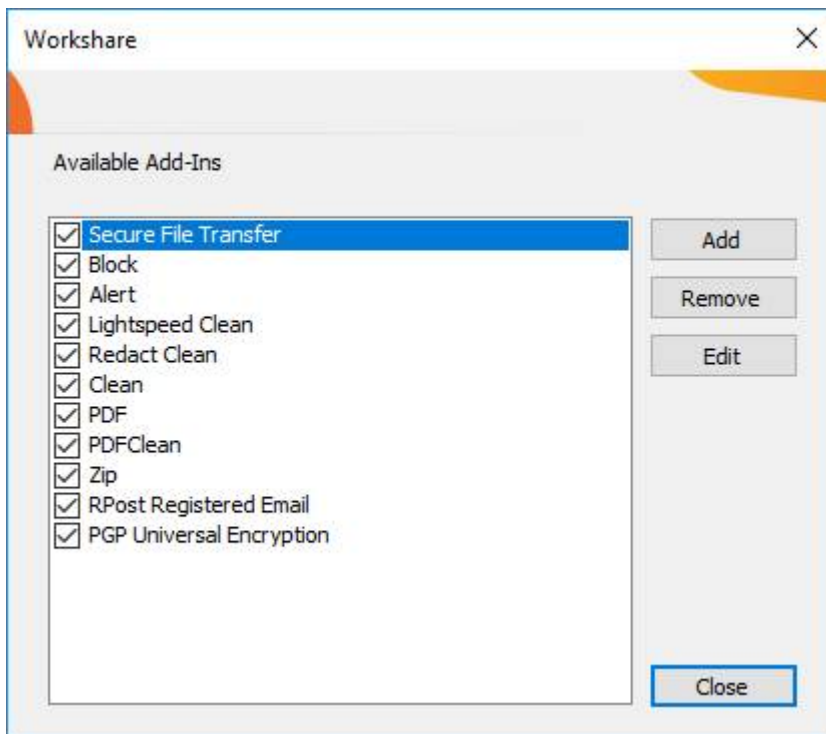
- Introducing the Actions Add-in Manager, page 90
- Adding New Actions, page 91
- Modifying Action Properties, page 92

Introducing the Actions Add-in Manager

The Add-In Manager enables you to edit the default actions provided with Workshare Protect as well as add third party actions. You can write your own custom actions using the Workshare Protect API (contact Workshare for further information).

To access the Add-in Manager:

From the *Tools* menu in the Workshare Policy Designer main window, select **Add-in Manager** and then **Actions**. The Policy Action Add-In Manager is displayed.



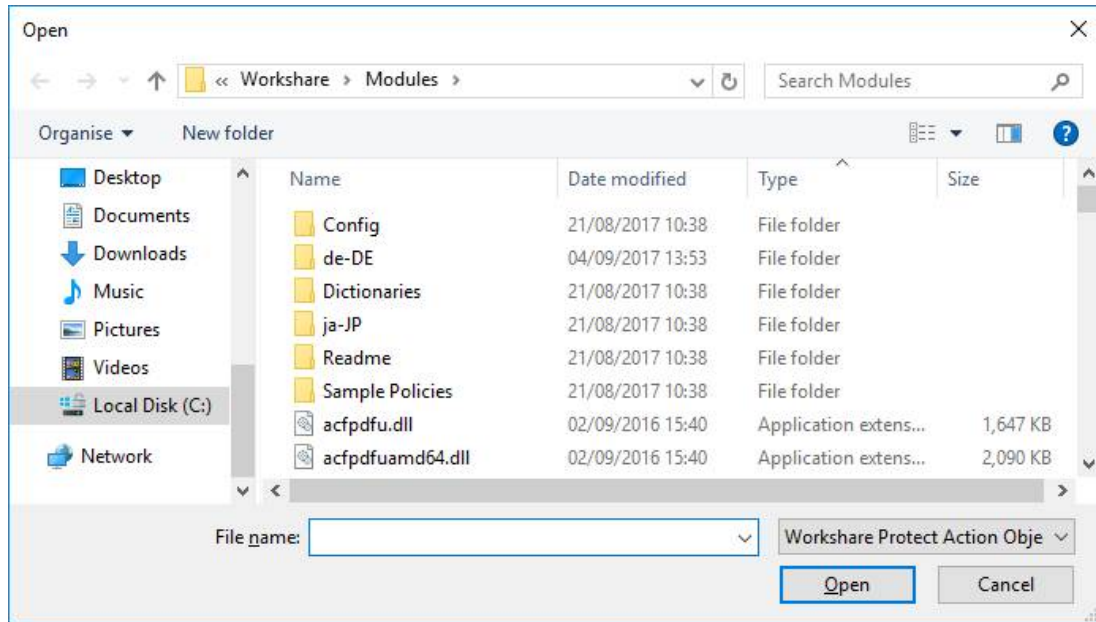
The currently defined actions are listed in their order of precedence.

Adding New Actions

Using the Action Add-In Manager, you can bring in your own action DLL files and have the action available in the Workshare Policy Designer. For more information on writing your own custom actions, contact Workshare for Workshare Protect API documentation.

To add a new action:

1. In the Policy Action Add-In Manager, click **Add**.



2. Browse to the location of your action DLL and click **Open**. The selected action is added at the bottom of the list of actions in the Policy Action Add-In Manager. You can then modify the default properties of the action.

Modifying Action Properties

Using the Actions Add-In Manager, you can modify the default settings of action properties.

To modify action properties:

In the Policy Action Add-In Manager, select the action to modify and click **Edit**. The *Action Detail* dialog is displayed.

The **Action Detail** dialog box is shown with the following sections:

- Action Name:** Unique Action Name: Clean
- Policy Support:** Please select which policies you would like this action to be available for.
 - ☐ Legacy Policy
 - ☐ Active Content Policy
 - ☒ Client Email Policy
 - ☐ Client Removable Media Policy
 - ☐ Desktop Content Discovery Policy
- File Type Support:** Please select which file types you would like this action to be available for.
 - ☒ .doc
 - ☒ .xls
 - ☒ .ppt
 - ☒ .docx
 - ☒ .docm
 - ☒ .dotx
 - ☒ .dotm
- Property Defaults:**


Available Action Properties	Default Value
Footnotes	True
Document Statistics	True
Built In Properties	True
Headers	True
Footers	True
Smart Tags	True
Template	True
Custom Properties	True

[Create a new custom property](#)
- User visibility:**
 - ☒ Allow this action to be processed transparently
 - ☐ Expand this action's first item when being displayed
- When this action is triggered:** Allow user to override it (it will be checked by default)

Buttons: OK, Cancel

You can modify the default settings of the properties. For example, you can deselect a file type in **File Type Support** so that the action is not available for all file types or you can add boilerplate text to the **Description** field.

Note: Before creating your own custom action, contact Workshare for information and assistance and support for this feature.

 Workshare Ltd.

© 2017. Workshare Ltd. All rights reserved.

Workshare Professional and Workshare DeltaView are registered trademarks of Workshare Ltd. Workshare Compare, Workshare Protect, Workshare 3, Workshare DeltaServer, SafetyGain, and the Workshare logo are trademarks of Workshare Ltd. All other trademarks are those of their respective holders.

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

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.

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