

# Workshare **Protect**

Policy - enforced Document Security for Microsoft

**4.5**

Workshare Protect 4.5 Quality Assurance Test Scripts

## **PROTECT 4.5 STABILITY TEST CASE**

Build	
Test Engineer	
Verified by	
Date	

### **Smoke/Stability Test Requirements:**

<b><i>Req Id</i></b>	<b><i>Test Requirement Description</i></b>	<b><i>Functional Area</i></b>
REQ1	Installation	INSTALL/UNINSTALL
REQ2	Workshare Protect icons	GUI
REQ3	Discover hidden data	HIDDEN DATA
REQ4	Add-in restrict document	SECURITY
REQ5	Add-in pdf document	PDF
REQ6	Scan document	HIDDEN DATA
REQ7	Batch Cleaning	HIDDEN DATA
REQ8	GUI	GUI
REQ9	Configuration settings	CUSTOMIZATION
REQ10	Attachment handling and	SECURITY

	sending e-mail	
REQ11	Attachment Options Dialog	EMAIL
REQ12	PDF attachment handling(Default Options)	SECURITY /PDF
REQ 13	Trace	CONTENT RISK
REQ14	Uninstalling the application	INSTALL/UNINSTALL

**Traceability Matrix:**

<i>Req ID</i>	<i>Test Requirement Description</i>	<i>Test Case ID</i>	<i>Description</i>
REQ1	Installation	1.0	Installing the application with a full license
REQ2	Workshare Protect icons	2.0	Checking for Workshare Protect icons in a Word document(.doc)
		2.1	Checking for Workshare Protect icons in excel sheet(.xls)
		2.2	Checking for Workshare Protect icons in PowerPoint Presentation(.ppt)
REQ3	Add-in discover hidden data	3.0	Tracking hidden data in a Word document (.doc)
		3.1	Tracking hidden data in Excel sheet (.xls)
		3.2	Tracking hidden data in a PowerPoint Presentation (.ppt)
REQ4	Add-in restrict document	4.0	Restricting a document
REQ5	Add-in PDF document	5.0	PDF word document
		5.1	PDF excel document

		5.2	PDF powerpoint document
REQ6	Scan functionality from standalone application	6.0	Scan document(s)
		6.1	Scan folder
		6.2	Scan email
REQ7	Batch Cleaning	7.0	Checking for meta data in multiple files
REQ8	GUI	8.0	Checking the graphical user interface
REQ9	Configuration settings	9.0	Customizing the configuration settings
REQ10	Attachment handling and sending email	10.0	Checking the attached document sent through e-mail for hidden data
REQ11	Attachment options dialog testing	11.0	Testing the application of settings to individual documents
		11.1	Testing convert to PDF
REQ12	Uninstallation of application	12.0	Ensuring application removed correctly

## Test Script

**Note: Before installing Protect.exe, open MS Word, Excel and PowerPoint once and close the documents.**

1.0 INSTALL AS ADMINISTRATOR (FULL LICENSE)			
1.0.1	Install as Administrator and enter license	<ul style="list-style-type: none"> <li>a. Check the Version ensure that the Build Version is displayed correctly</li> <li>b. Once the user clicks on the button to use start using 'Workshare Protect', the application should launch 'Scan your documents' pop up</li> <li>c. The batch clean functionality should be available under the file menu in the application.</li> </ul>	
1.0.2	Log on as a restricted user, launch protect	<ul style="list-style-type: none"> <li>a. The scan documents dialog should be displayed</li> </ul>	

**Pre-conditions: Execute all of the following test scripts after logging in as 'Normal' User.**

2.0 WORKSHARE PROTECT ICONS(.DOC)			
2.0.1	Open a saved word document	The document should open with 'Publish to PDF', 'Publish to PDF', 'Discover Content Risk' and 'Restrict Document' icons in the toolbar	
2.1 WORKSHARE PROTECT ICONS (.XLS)			

2.1.1	Open a saved Excel document	The document should open with 'Publish to PDF', 'Publish to PDF', 'Discover Content Risk' and 'Restrict Document' icons in the toolbar	
<b>2.2 WORKSHARE PROTECT ICONS(.PPT)</b>			
2.2.1	Open a saved PowerPoint document	The document should open with 'Publish to PDF', 'Publish to PDF', 'Discover Content Risk' and 'Restrict Document' icons in the toolbar	
<b>3.0 ADD-IN DISCOVER HIDDEN DATA(.DOC)</b>			
3.0.1	Open a saved word document and click to Discover Content Risk using the Protect Add-in in Word Toolbar or the option from the File Menu	This document may contain any of these elements: Track Changes, Comments, Hidden Text, White Text, Small Text ( <i>Only 1pt, 2pt, 3pt, 4pt and not for 1., pt, 2.5pt, 3.5pt</i> ), Footnotes)/ Endnotes ( <i>Will only be discovered if the options is ticked in Administration Settings in the Configuration, Versions, Auto versioning, Routing Slip, Custom Properties, Document Statistics, Previous Authors, Macros, document Reviewers, Field Codes, Document Variables, Build in Properties, Templates, Smart Tags</i>	
3.0.2	Clean elements according to High/ Medium/ Low Settings)	Ensure elements have been cleaned according to the specified settings	
<b>3.1 ADD-IN DISCOVER HIDDEN DATA(.XLS)</b>			
3.1.1	Open a saved Excel document and click to Discover Content Risk using the Protect Add-in in Word Toolbar or the option from the File Menu	This document may contain any of these elements: Track changes, Comments, Hidden Text, White Text, Small Text ( <i>Only 1pt, 2pt, 3pt, 4pt and not for 1., pt, 2.5pt, 3.5pt</i> ), Footnotes)/ Endnotes ( <i>Will only be discovered if the options is ticked in Administration Settings in the Configuration, Versions, Auto versioning, Routing Slip, Custom Properties, Document Statistics, Previous Authors, Macros, document Reviewers, Field Codes, Document Variables, Build in Properties, Templates,</i>	


		Smart Tags	
3.1.2	Clean elements according to High/ Medium/ Low Settings)	Ensure elements have been cleaned according to the specified settings	
<b>3.2 ADD-IN DISCOVER HIDDEN DATA(.PPT)</b>			
3.2.1	Open a saved PowerPoint document and click to Discover Content Risk using the Protect Add-in in Word Toolbar or the option from the File Menu	This document may contain any of these elements: Track Changes, Comments, Hidden Text, White Text, Small Text ( <i>Only 1pt, 2pt, 3pt, 4pt and not for 1., pt, 2.5pt, 3.5pt</i> ), Footnotes)/ Endnotes ( <i>Will only be discovered if the options is ticked in Administration Settings in the Configuration, Versions, Auto versioning, Routing Slip, Custom Properties, Document Statistics, Previous Authors, Macros, document Reviewers, Field Codes, Document Variables, Build in Properties, Templates, Smart Tags</i>	
3.2.2	Clean elements according to High/ Medium/ Low Settings)	Ensure elements have been cleaned according to the specified settings	
<b>4.0 ADD-IN RESTRICT DOCUMENT</b>			

4.0.1	Launch a saved word document and click on the Word Add-in for Document Restrictions	Check documents should by default is set to No restriction	
4.0.2	Set the document restriction to No Restriction/External/full restriction. Apply the change	Ensure that when a document is set to No Restriction/External/full restriction the change is applied as per the specified customization	
4.0.3	Perform steps 4.0.1 and 4.0.2 on a saved Excel and PowerPoint document	Ensure that the results are as expected	
<b>5.0 PDF FROM OPEN WORD DOCUMENT (The option must be enabled in Protect Config Manager 'Enable convert to PDF within MS Office')</b>			
5.0.1	Launch a saved word document	Ensure the PDF icon is present in the toolbar	
5.0.2	Select to PDF the document	The Protect PDF dialog should be displayed.	
5.0.3	Leave the options as the default and select "OK"	A local file store prompt should be displayed.	
5.0.4	Select a location to save the document and press "OK"	The pdf should be generated; after the process is complete a dialog should be displayed prompting the user to view the PDF document. Select "yes" the PDF should be launched correctly.	

<b>5.1 PDF FROM OPEN EXCEL DOCUMENT</b>			
5.1.1	Launch a saved Excel document	Ensure the PDF icon is present in the toolbar	
5.1.2	Enter some text into excel and save the document. Enter some more text (the status of the document is then saved and dirty). Select the PDF button	The Protect PDF dialog should be displayed.	
5.1.3	Set some security options and press "OK"	A local file store prompt should be displayed.	
5.1.4	Select a location to save the document and press "OK"	The PDF should be generated; after the process is complete a dialog should be displayed prompting the user to view the PDF document. Select "no" focus should be returned to Excel.	
5.1.5	Launch the saved PDF	Ensure the security settings are correct (ctrl+d) to view Adobe security	
<b>5.2 PDF FROM OPEN POWERPOINT DOCUMENT</b>			
5.2.1	Launch a saved PowerPoint document	Ensure the PDF icon is present in the toolbar	

5.2.2	Enter some text (do not save). Select the PDF option from the file menu.	The Protect PDF dialog should be displayed.	
5.2.3	Set all the security options and press "OK"	A local file store prompt should be displayed.	
5.2.4	Select a location to save the document and press "OK"	The PDF should be generated; after the process is complete a dialog should be displayed prompting the user to view the PDF document. Select "yes", the document should be launched in Adobe. Ensure the pdf security is correct.	
<b>6.0 SCAN DOCUMENT</b>			
6.0.1	Launch Workshare Protect application, select 'Scan' from File Menu/Scan icon in the toolbar	Ensure that Workshare Protect window with 'Scan Your Files' and 'Scan Your Emails' options are displayed	
6.0.2	Click on 'Scan Your Files' link and select a file to scan	Ensure that the browse window is displayed and after selecting a file, a report is generated with hidden data	
<b>6.1 SCAN FOLDER</b>			
6.1.1	Launch Workshare Protect application, select 'Scan' from File Menu/Scan icon in the toolbar	Ensure that Workshare Protect window with 'Scan Your Files' and 'Scan Your Emails' options are displayed	
6.1.2	Click on 'Scan Your Files' link and select a folder to scan	Ensure that a report is generated with all hidden data identified for all supported documents within the folder.	

<b>6.2 SCAN EMAIL</b>			
6.2.1	Launch Workshare Protect application; select 'Scan' from File Menu/Scan icon in the toolbar. From the Scan dialog select "scan your email"	A select folders dialog should be displayed; the file structure of the dialog should match that of the relevant email client	
6.2.2	Select an email folder and select "OK"	The relevant email folder should be displayed and a report should be generated showing all hidden data in supported document types	
<b>7.0 BATCH CLEANING</b>			
7.0.1	Select multiple documents and folders (can be .doc/.rtf/.ppt/.xls) for Batch Clean	Check if Batch Cleaning cleans metadata according to the settings	
<b>8.0 GUI</b>			
8.0.1	Tool tip text, Help, Branding and short cut keys	Ensure the tool tip text, Branding and short cut keys are as expected and in place throughout the product	
<b>9.0 CONFIGURATION SETTINGS</b>			
9.0.1	Launch Workshare Protect and select 'Configuration' option from File Menu or click on 'Configure' from the toolbar	Ensure that 'Saving/Loading configuration' window is displayed with options in the left pane	
9.0.2	Select an option from the left pane and change the settings	Ensure that the changes are applied accordingly	
<b>10.0 ATTACHMENT HANDLING AND SENDING E-MAIL</b>			

10.0.1	Attach .doc/.rtf/.dot/.xls/.ppt documents to an email and send it	Ensure that the Attachment Options Dialog is displayed and with 'Action Summary' view defaulted. There should also be a Hidden Data tab and PDF tab	
10.0.2	As a reviewer, open the sent mail	Ensure that the hidden data has been cleaned according to the settings	
<b>11.0 ATTACHMENT OPTIONS DIALOG (DEFAULT OPTIONS)</b>			
11.0.1	Send documents to an external user (rtf, doc, xls, ppt, dot and PDF)	<p>An attachments options dialog should be displayed:</p> <ol style="list-style-type: none"> <li>Ensure that all documents are displayed in the left pane and are selected (the PDF should be displayed as an unsupported file type).</li> <li>Ensure the dialog appears with the options as shown in the attached file.</li> </ol>  <p>attachoptions.rtf</p>	
11.0.2	Select a single document and select "View Risk Report"	An accurate report should be generated and launched in a viewer application.	
11.0.3	Highlight a single document and preview it (double click)	The document should be launched in its native application with the metadata cleaned according to the settings. Close the document.	
11.0.4	Select all the documents, check to the option to produce a confirmation report and press "Send"	<ol style="list-style-type: none"> <li>All the attachments should be cleaned according to the default settings.</li> <li>A confirmation cleaning report should be generated showing all the operations carried out on the document</li> </ol>	

11.0.5	Launch the documents from the email in the inbox of the recipient	Ensure that the metadata was cleaned according to the settings.	
11.0.6	Right click send a document by email, address to an internal recipient	The attachment options dialog should not be displayed and no metadata should be cleaned (default settings)	
<b>12.1 PDF ATTACHMENT HANDLING</b>			
12.1.1	Send documents to an external user (rtf, doc, xls, ppt, dot and pdf)	The attachments options dialog should be displayed	
12.1.2	Highlight one or more of the documents and select the convert to PDF option. Select the "Send"	<p>The convert to PDF progress dialog should be displayed.</p> <ul style="list-style-type: none"> <li>a. The selected documents should be cleaned of selected metadata and converted into PDF format</li> <li>b. The remaining documents should be cleaned but not converted to PDF</li> </ul>	
<b>13.0 TRACE</b>			
13.0.1	Open a saved word document	Ensure that the Trace icon changes according to the type of risk elements present in the document. (Green for Low risk elements, Yellow for Medium risk elements and Red for High risk elements)	
13.0.2	Double click on the trace icon in the sys tray	Ensure that a report is generated with accordingly, all the high, medium and low risk elements are reported as expected. Also ensure that the Content is discovered as expected. (If present)	
<b>13.1 EXCEL</b>			
13.1.1	Open a saved Excel document	Ensure that the Trace icon changes according to the type of risk elements present in the document. (Green for Low risk elements, Yellow for Medium risk	

		elements and Red for High risk elements)	
13.0.2	Double click on the trace icon in the sys tray	Ensure that a report is generated with accordingly, all the high, medium and low risk elements are reported as expected. Also ensure that the Content is discovered as expected. (If present)	
<b>14.0 UNINSTALLATION OF PROTECT</b>			
13.1.1	Open a saved PowerPoint document	Ensure that the Trace icon changes according to the type of risk elements present in the document. (Green for Low risk elements, Yellow for Medium risk elements and Red for High risk elements)	
13.0.2	Double click on the trace icon in the sys tray	Ensure that a report is generated with accordingly, all the high, medium and low risk elements are reported as expected. Also ensure that the Content is discovered as expected. (If present)	
<b>14.0 UNINSTALLATION OF PROTECT</b>			
14.0.1	From the "add remove programs" dialog select to "remove" workshare protect.	<p>After a "yes" "no" confirmation dialog the un-installation should proceed and a notification presented when it is completed. Only the following should be left behind after the uninstallation has completed:</p> <ul style="list-style-type: none"> <li>a. Installation directory "C:\Program Files\Workshare\modules" containing <ul style="list-style-type: none"> <li>• Metawall.lic</li> <li>• Install.txt</li> </ul> </li> <li>b. Any shortcuts created by the user</li> <li>c. The options and settings xml files in the following locations: <ul style="list-style-type: none"> <li>• C:\documents and settings\<users>\application data\workshare\workshare</users></li> </ul> </li> <li>d. The following files in the "C:\documents and settings\All Users\Application Data\Workshare"</li> </ul>	

		<p>directory:</p> <ul style="list-style-type: none"><li>• Metadatasecurityratings.xml</li><li>• Metadtasecurityratings.xsd</li><li>• Settings.xml</li></ul>	
--	--	---	--