GUIDE

Workshare Protect

Installation Guide

Workshare

Company Information

Workshare Protect Installation Guide

Workshare Ltd. (UK)
20 Fashion Street
London
E1 6PX
UK

Workshare Inc. (USA)
208 Utah Street, Suite 350
San Francisco
CA 94103
USA

Workshare Website: www.workshare.com

Trademarks

Trademarked names appear throughout this guide as well as on other parts of the Workshare Protect CD. 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.

Disclaimers

The authors/publishers of the Workshare Protect Installation Guide and 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 the Workshare Protect Installation 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.

Copyright

Useful Information

The following information may be useful.

Additional Documentation

In addition to this guide, you should also have the Workshare Protect User Guide and the Workshare Protect Getting Started Guide. If you are interested in the concepts behind Workshare Protect and other products from Workshare, you can read white papers and download product demos from www.workshare.com.

Contacting Technical Support

To contact Workshare support, please refer to: http://www.workshare.com/support/.

Knowledge Base

There is now a Workshare knowledge base with many solutions to common problems. To search this knowledge base, follow these steps:

1. Go to www.workshare.com.
2. Select **Support**.
3. Enter keywords (for example, collaboration tool) and click **Find Article**. A list of results is displayed.
4. Click a link to display the details.

Feedback

If you have any comments about Workshare Protect — ideas for improvements, new features or anything at all — please feel free to email our Product Management team at: feedback@workshare.com.

Table of Contents

Chapter 1. Installation Overview

This chapter introduces Workshare Protect providing an overview of the installation of Workshare Protect as well as a list of system requirements. It includes the following sections:

- **What is Workshare Protect?**, below, introduces Workshare Protect and its key functionality.
- **Workshare Protect Functionality**, page 11, describes the different functionality available in Workshare Protect.
- **System Requirements**, page 12, describes the system attributes required in order to install and run Workshare Protect.
- **Installation Best Practice Guidelines**, page 13, describes the recommended installation and deployment procedure for Workshare Protect.
- **Important Information**, page 17, provides important information that should be read before installing, configuring and deploying Workshare Protect.
- **Licensing**, page 21, provides information about the various licenses available for Workshare Protect.

What is Workshare Protect?

Workshare Protect is seamlessly integrated with Microsoft Office and automatically enforces company security policy at end-user workstations. Rather than simply block information flow, Workshare Protect warns and educates users in real-time about sensitive information and, if authorized, lets users decide how to treat the content. Workshare Protect provides:

- **Hidden Data/Metadata Removal**
  - Policy driven content risk management
  - Discovery and removal of hidden data and visible content leaks
  - Complete metadata protection for Microsoft Office documents
- **Tamper-Proof PDF Creation**
  - Converting any document to Workshare's secure PDF from any application
  - Ensuring flexible publishing and complete PDF security options
  - Enforcing automatic conversion of documents to secure PDF before they can be emailed
- **Stopping of Violations in Real Time**
  - Flagging policy violations in real time using smart tags
  - Educating users about content to avoid with active task bar notifications
  - Enabling users to fix potential problems with manual redaction options
  - Password-protecting documents or restricting them from being sent externally, or at all.
- **Content Protection and Control**
  - Content analysis and data leak prevention
  - Automatically stopping leaks of intellectual property at their origin
  - Keeping data safe and secure from embarrassing public disclosures
  - Monitoring all communications at the client level
  - Providing alerts for data in use, at rest, and in motion—even when disconnected from the network

For users who have Workshare Device Protector (powered by Safend) or Safend Encryptor installed, Workshare Protect provides the following:

- **Monitoring and blocking content on USB and other removable media**

  Safend policies define which files downloaded to external storage devices should be inspected and these files are then sent to the Workshare Protect client for inspection, where Workshare policy determines whether the files are blocked or the user alerted to sensitive information.

  Refer to Safend Protector documentation for further details.

- **Full disk encryption**

  Safend Encryptor provides a hard disk encryption solution that leverages the security of full-disk encryption and the flexibility of file-based encryption to protect sensitive data residing on desktops and laptops.

  Refer to Safend Encryptor documentation for further details.

Workshare Protect Functionality

Discovering Content Risk

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

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

- **Content Risk Reports**: Workshare Protect integrates with Microsoft Office providing an option to display a comprehensive report of all the content risk in a document while it is open in Microsoft Word, Excel and PowerPoint. Content risk is displayed according to its risk level (high, medium, low). Selected content risk can then be automatically removed from the document as required.
- **Email Protection**: Workshare Protect prevents users from accidentally emailing confidential information by alerting users before the email is sent when an email or its attachment breaches security policies. Depending on the actions defined for policy breaches, emails may be blocked or sensitive data removed. Security policies can specify different actions when a document is sent internally or externally. For example, it may not be acceptable for hidden server names and users details to be included in documents sent externally, but it may be fine to leave those details in documents sent within an organization.
- **Real-Time Alerts**: When open Microsoft Office documents trigger a breach of a security policy with an Active Task Bar action defined, a real-time policy alert is displayed in the bottom right of the screen notifying the user of the policy breach. When open Microsoft Office documents trigger a breach of a security policy with a Smart Tag action defined, a smart tag (a purple dotted line beneath the text) notifies the user of the policy breach.

In Workshare Protect, content risk protection is provided using security policies. Workshare Protect comes with a pre-defined default security policy which you can edit if required using the Workshare Protect Configuration Manager. For a detailed description of what the default policy covers, refer to *Appendix A: Workshare Protect Default Policy*.

> ***Note:*** *If Workshare is integrated with the Workshare Device Protector (powered by Safend), Workshare offers enhanced content inspection for files transferred to removable media devices. Refer to the Safend Protector documentation for further information.*

Manual Redaction

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

Document Classification

Workshare Protect enables you to restrict access to sensitive business documents by classifying documents. This classification can prevent documents from being emailed either to any user, or to external users. Workshare Protect provides the following default classification levels:

- For Internal Use
- Confidential
- Highly Confidential
- External Restriction
- Full Restriction

PDF Conversion

Workshare Protect enables you to quickly and easily convert documents into PDF (Portable Document Format) from any application. This Workshare Protect functionality is available from within Microsoft Word, Excel and PowerPoint environments, by right-clicking closed Microsoft Word, Excel and PowerPoint files on your desktop or DMS and by printing any file to the Workshare PDF printer.

System Requirements

You should check that your system meets the following requirements:

Recommended System Requirements	2.2GHz Intel Core 2 Duo processor or equivalent 2GB RAM 2GB free disk space

Compatibility

Workshare Protect is compatible with the following:

Operating System:

- Microsoft Windows XP (SP3 and above)
- Microsoft Windows Vista (32 bit and 64 bit) – UAC disabled

> ***Note:*** *When you are integrating Workshare Protect with Workshare Device Protector on Microsoft Windows Vista, the requirement is Microsoft Windows Vista (32 bit) SP1 and above.*

- Microsoft Windows 7 (32 bit and 64 bit)
- Microsoft Windows 2003 Server (32 bit and 64 bit)
- Microsoft Windows 2003 R2 Server (32 bit and 64 bit)
- Microsoft Windows 2008 Server (64 bit)
- Microsoft Windows 2008 R2 Server (64 bit)

Citrix (deployed Published Applications and Published Desktop):

> ***Note****: Check with your Citrix vendor about which Windows operating system supports your Citrix.*

- Citrix Presentation Server 4.0 and 4.5
- Citrix XenApp 5.0

Microsoft Office System:

- Microsoft Office 2007 (No SP, SP1 and SP2)
- Microsoft Office 2003 (No SP, SP1, SP2 and SP3)
- Microsoft Office XP (SP2 and SP3)

> ***Note:*** *You should have a* ***full*** *installation of Microsoft Word, Excel and PowerPoint. Microsoft Office should be installed on a per machine basis.*

Email System:

- Microsoft Outlook 2007 (No SP, SP1 and SP2)
- Microsoft Outlook 2003 (No SP, SP1, SP2 and SP3)
- Microsoft Outlook XP (SP2 and SP3)
- IBM Lotus Notes 7.03 to 8.5.1

> ***Note:*** *You should have a* ***full*** *installation of Microsoft Outlook. It should be installed on a per machine basis.*

Microsoft SharePoint:

- Microsoft Office SharePoint Server 2007

Installation Best Practice Guidelines

This guide will take you through a typical Workshare Protect installation. The general steps involved are as follows:

1. Install Workshare Protect on a single workstation (described in *Chapter 2: Installation*).
2. Configure Workshare Protect, as you want it to work in your organization (described in *Chapter 3: Configuration*).
3. Save the configuration in a configuration (INI) file to a network share location (described in *Saving Configuration Files* in *Chapter 3: Configuration*).
4. Deploy Workshare Protect across your network, specifying the LICFILE parameter so that it is licensed and the INIFILE parameter so that it is configured uniformly across your organization (described in *Chapter 5: Network Deployment*).

It is recommended that you follow the guidelines listed below when installing Workshare Protect to ensure a smooth and trouble-free installation:

- Ensure that your system meets the minimum requirements for Workshare Protect shown on page 10.
- Ensure that all important data is backed up prior to installation.
- Close all other applications before installing Workshare Protect.
- Elevated/administrator privileges are required to install Workshare Protect.
- Only recommended installation properties such as INSTALLDIR should be altered. Any major changes to the installation procedures may cause issues with the software.
- Workshare MSI files should not be directly edited. Changes can be applied via a transform file (.mst) or other method of applying properties such as command line parameters.
- Transform files may be created via any third party software that entirely supports Windows Installer technology.
- Workshare MSI files should not be repackaged. Certain custom actions that are contained in the original MSI file may be missed and may also prevent future upgrades.
- Workshare MSI files should not be patched with in-house authored MSP files as this may cause future upgrade issues and system instability.
- Additional customer specific files and Registry keys may be deployed alongside Workshare software as long as they do not interact or replace any files or Registry keys belonging to the product.
- No additional third party software should be bundled into any Workshare MSI.

If you have any queries about the installation of Workshare Protect that are not dealt with in this Administration Guide, please contact Workshare Customer Service (details on page 3).

Workshare Protect Installation Files

This section describes the Workshare Protect executables, Windows Installer Packages and shared components.

Executables

Workshare Protect is installed using a single, downloadable self-extracting executable called **WorkshareProtect-9800.xxx.exe**.

On a single workstation, the easiest way to install Workshare Protect is to simply run the install EXE file and answer any questions asked. Where an installation per computer is not feasible, you can deploy Workshare Protect to multiple workstations using methods described in *Chapter 5: Network Deployment*.

Prerequisite Components

The prerequisites for Workshare Protect depend on the version of the operating system and the version of Microsoft Office. They are described in the following table. Prerequisites for other versions of Workshare Protect may be slightly different.

Workshare Protect is a native x86 application. It normally requires the x86 prerequisites for proper operation. The exception is the Microsoft .NET Framework which must have the appropriate x86/x64 version installed.

Prerequisite	Version	OS	Office	Notes
Windows Installer	3.1.0.0	Windows XP, Server 2003	NA	
Microsoft .NET Framework 3.0	3.0.4506.30	Windows XP, Server 2003	NA	Microsoft .NET Framework 3 contains Microsoft .NET Framework 2 and MSXML 6.0.
KB908002 - Shared Add-in Support Update for Microsoft .NET Framework 2.0	1.0.0	NA	All versions	This KB is required for Microsoft Office to load .NET add-ins.
MSXML 6.0	NA	NA	NA	This prerequisite is installed by the Microsoft .NET Framework 3 install.
Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x86)	8.0.5193	All (including x64 versions)	NA	
Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x64)	8.0.5192	x64 OS versions	NA	The right-click handler is written in x64 code and requires this prerequisite.

Prerequisite	Version	OS	Office	Notes
Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x86)	9.0.30729.4148	All (including x64 versions)	NA	
Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x64)	9.0.30729.4148	x64 OS versions	NA	The right-click handler is written in x64 code and requires this prerequisite.
Microsoft Report Viewer (x86)	8.0.50727.42	All	NA	
KB907417 – Update for Office 2003	1.0.0	NA	Office 2003	
KB935514 – Update for Office 2007	1.0.0	NA	Office 2007 pre SP1 only	
Microsoft Office System Primary Interop Assemblies (PIA)	12.0.4518.1014	NA	Office 2007	
Open XML Format SDK	1.0.1825	All	NA	
Windows Installer for Server 2003 (x64)	3.1	Windows Server 2003 x64	n/a	http://www.microsoft.com/downloads/details.aspx?FamilyId=8B4E6B93-1886-4D47-A18D-35581C42ECA0&displaylang=en
Windows Installer for Server 2003 (x86)	3.1	Windows Server 2003 x86	n/a	http://www.microsoft.com/downloads/details.aspx?FamilyId=8B4E6B93-1886-4D47-A18D-35581C42ECA0&displaylang=en

***Note:** Windows Installer and Microsoft .NET Framework should be installed first. The other prerequisite components can be installed in any order.*

For further information about each prerequisite, refer to *Appendix D: Workshare Protect Prerequisites*.

Windows Installer Packages

If you need to extract the MSI it can be extracted from the executable using third party zip tools, and run directly. The MSIs that can be extracted from the executable files are as follows:

- **Workshare PDF Converter Version 5.0.159**
- **Workshare Protect Client** - WorkshareProtect.msi installs Workshare Protect.

If you install using an extracted MSI, you must first install all the prerequisite components described above.

Note: *Please ensure that all the prerequisites and the MSIs are installed in the same user context.*

Workshare PDF Publisher

When Workshare Protect is installed it creates a printer called **Workshare PDF Publisher** in the user's **Printers** folder. This is the printer that Workshare Protect uses to convert documents to PDF.

Important Information

Upgrading from Workshare Protect

Users who are upgrading from earlier versions of Workshare Protect should not re-use their configuration (INI) files. Several settings have changed, which makes previous INI settings invalid. If INI files from earlier versions of Workshare Protect are used, errors may be encountered. Users should create new INI files for distribution using the Workshare Configuration Manager from Workshare Protect 5.2 SR3.

When upgrading from earlier versions of Workshare Protect, the general configuration settings are carried over to Workshare Protect 5.2 SR3. See the *Workshare Protect Release Notes* for further information.

System and Diagnostic Checks

System Checks

Workshare Protect performs the following system checks during the installation process:

- The version of Microsoft Windows operating system
- The amount of available memory
- The availability of Active Template Library 8.0
- The availability of Microsoft Framework Classes 8.0
- The following applications are closed: Microsoft Word, Microsoft Outlook, IBM Lotus Notes, IBM Lotus Notes Login, Hummingbird DOCS Open, Interwoven, Hummingbird
- Microsoft Word is version 10 or above

- Microsoft XML is version 6 or above
- Microsoft Internet Explorer is version 5.5 or above
- Microsoft .NET Framework is version 3.0

Diagnostic Checks

Workshare Protect performs the following diagnostic checks during the installation process:

- There is a default document provider specified in settings.xml
- The document template files exist where specified
- Microsoft Office has registered Workshare Protect Add-Ins
- The options.xml and settings.xml files exist where specified
- The Protect COM Registry entries exist and point to a valid file
- All files in the ShippingManifest.xml file exist
- The current user Application Folder entry in the Registry is valid
- The current code page is valid
- Other email system-specific checks are successful

Workshare Configuration Assistant

The Workshare Configuration Assistant (WCA) is a program that completes the Workshare Protect installation process. The WCA is not optional as it performs actions that are required to correctly install Workshare Protect. The install process automatically runs the WCA silently.

Re-Running the WCA

Following installation, the WCA can be run as a separate executable for any of the following reasons:

- To repair or continue a previously incomplete installation
- To distribute a configuration (INI) file
- To update an installation

When re-run, the WCA provides information on the progress of installation and any necessary messaging if any problems are encountered. If a problem is encountered, the user can access the online Workshare knowledge base which provides an extended description and, where possible, a solution to resolve the problem.

The executable is named **WMConfigAssistant.exe** and is found in the **Modules** folder of the Workshare Protect installation directory. To be run, the WCA requires administration rights to the workstation.

The WCA executable is run from the command line, from within a DOS window or using a batch (.bat) file. This should only be attempted by the network administrator or other qualified personnel. The WCA can be run silently, without any user interface and quietly, with a reduced user interface.

The WCA is also available form the Start Menu: Start > Programs > Workshare > Workshare Configuration Assistant.

To run the WCA from the command line, the following syntax should be used:

```
"C:\Program Files\Workshare\Modules\WMConfigAssistant.exe" /INSTALL /SILENT
/INIFILE="\\InstallMachine\Workshare\Workshare.ini"
/LOGFILE="\\InstallMachine\Workshare\Workshare.log"
```

Where the switches can be:

Switch	Value
SILENT	Indicates that the WCA is to be run silently, with no user interface.
QUIET	Indicates that the WCA is to be run with a reduced user interface.
INIFILE	Name and location of the configuration file. For example, **INIFILE="\\server\share\inifile.ini"**. The specified INI file will be loaded to the **Modules\Config** folder of the Workshare Protect installation directory. For further information on the INI file, refer to *Chapter 3: Configuration*.
LOGFILE	Name and location of the WCA log file. For example, **LOGFILE="\\server\share\logfile.log"**. The log file can either be stored at a shared location or stored locally on the workstation. If a location is not specified for the log file it will be written to the local TEMP folder. By default the log file is named **WorkshareConfig.log**. The WCA log file will provide details of all the steps the WCA has taken and can be passed to Workshare if any difficulties are encountered. The log file is appended to, not overwritten, in order to retain all logged information. Therefore the latest details will be at the end of the log file.
LICFILE	Name and location of the license file. For example, **LICFILE="\\server\share\Workshare.lic"**. The specified LIC file will be copied to the **Modules** folder of the Workshare Protect installation directory.
NOTESINIFILE _PATH	Location of the notes.ini file. This should be specified in non-standard IBM Lotus Notes environments to ensure that Workshare components are added correctly to the INI file by the install.

Note: *The command must be entered on one line. You can use INSTALL, UNINSTALL, REINSTALL or REPAIR as the preceding switch. The use of " " should be used where there is character spacing in file paths.*

Workshare Menu

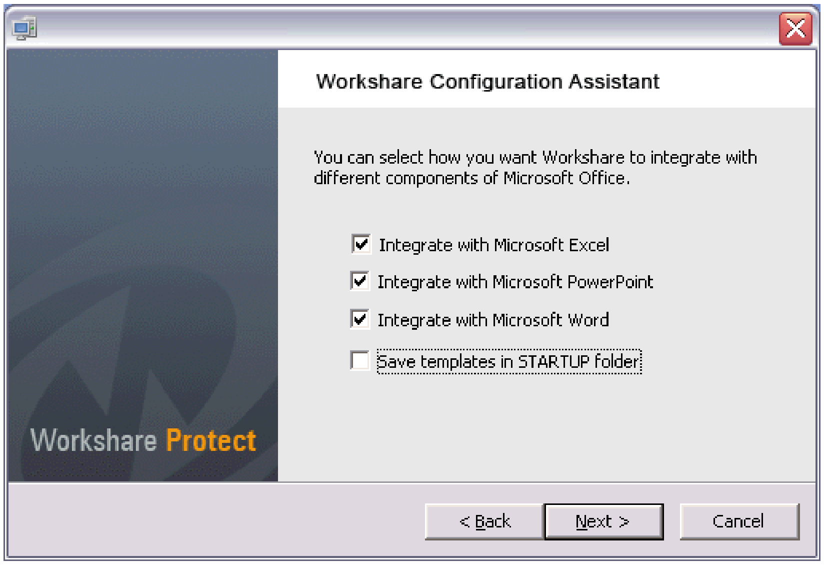
(This section is only relevant for users working with Microsoft Office 2003/XP.)

The Workshare menu is installed as a template called _Workshare3.dot. If you need to change the location of the Workshare menu, open _Workshare3.dot located in the **Modules** folder of the Workshare Protect installation directory. In the template file, move the Workshare menu to the position in the menu bar required and save the template.

If for any reason Workshare Protect is unable to display the Workshare menu when opening Microsoft Word, Workshare Protect will alert you to the problem and ask if you would like Workshare Protect to repair the problem. You may lose menu customizations when Workshare Protect repairs the problem.

Workshare Microsoft Office Integration

Workshare Protect is installed with Microsoft Office integration. If you want to change the integration of Workshare Protect with Microsoft Office applications, re-run the Workshare Configuration Assistant (described on page 18).



Workshare Configuration Assistant

You can select how you want Workshare to integrate with different components of Microsoft Office.

☑ Integrate with Microsoft Excel

☑ Integrate with Microsoft PowerPoint

☑ Integrate with Microsoft Word

□ Save templates in STARTUP folder

By deselecting the checkboxes, you can configure Workshare Protect to run without Microsoft Office integration. For example, by deselecting **Integrate with Microsoft Word**, there will be no Workshare Panel or Workshare menu/tab available in Microsoft Word. In this case, the metadata removal functionality is only available when sending emails. Additionally, you can select the **Save templates in STARTUP folder** to save the Workshare templates to the Microsoft Word STARTUP folder.

> ***Note***: *In command line installations, Microsoft Office integration is installed by default. The* ***Save templates in STARTUP folder*** *option can be turned on by creating the following Registry key:* ***SaveTemplatesToStartupFolder*** *with a DWORD value of* ***1*** *in the following Registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Workshare\Framework\Settings. You must create this Registry key before running the Workshare Protect installer.*
>
> *For further information about Microsoft Office integration in command line installations, see page 78.*

Configuration (INI) File

Workshare Protect settings can be distributed using a configuration (INI) file. The INI file encapsulates all the Workshare Protect configuration settings stored as XML data. Do not manually edit this file for any reason.

Using a configuration file, you can establish a global set of Workshare Protect parameters that can be used to standardize the use of Workshare Protect across your organization. The configuration file can be called anything as long as it has an INI extension and is placed in the **Config** folder of the Workshare Protect installation directory.

The configuration file is created using the Workshare Configuration Manager, which is accessed from the Options page of the Workshare Panel.

For a full description of the Workshare Protect configuration parameters and the Workshare Configuration Manager, refer to *Chapter 3: Configuration*.

Licensing

Workshare Protect can be licensed during installation or after installation. Licensing is effected using an authorization code or a license file issued by Workshare Ltd. Either or both of these can be used to license Workshare Protect.

There are several different license types, as follows:

Full Permanent License Issued to end users who have purchased a Workshare application. This license provides full access to the application as well as integration with a specified Document Management System. This license enables the Review and Audit, Compare and Protect modules.

Full Permanent License Issued to end users who have purchased a Workshare application. This license provides full access to the application as well as integration with a specified Document Management System (Interwoven, Hummingbird or SharePoint). This license enables the Review and Audit, Compare and Protect modules.

1, 2 3 Term License This license is the same as the permanent license except it is valid for a specific period (one, two or three years) and not permanently.

Temporary License Issued to end users who have purchased a Workshare application, as a form of interim licensing. If required, this type of license can be used prior to delivery of a permanent license.

Evaluation License Valid for a specified period of time, for potential users currently evaluating the software.

Demo/Trial License Valid for 14 days to enable users to try the software. Users are reminded on a daily basis how many days are left to run of the trial period.

Chapter 2. Installation

Workshare Protect can be installed on a single workstation or deployed across a network.

As part of the installation process, the WCA (see page 18) checks the configuration of your system and guides you through the licensing of Workshare Protect.

This chapter describes the installation and licensing procedure. It includes the following section:

- **Installing Workshare Protect**, below, describes the step-by-step procedure required to install Workshare Protect on a single workstation.
- **Uninstalling Workshare Protect**, page 25, describes how to uninstall Workshare Protect.
- **Licensing**, page 25, describes how to license Workshare Protect.

The procedure for installing Workshare Protect across a network is described in *Chapter 5: Network Deployment*.

Installing Workshare Protect

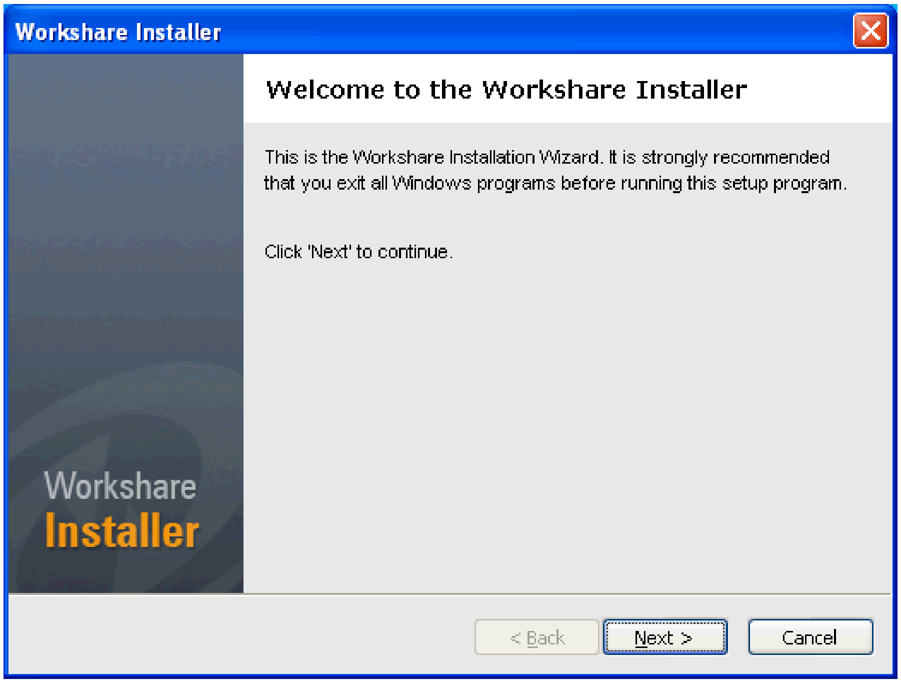
The following procedure explains how to install Workshare Protect on a single workstation. Before beginning the installation procedure, make sure that all other programs are closed and disable any anti-virus software.

The installation of Workshare Protect installs the following:

- Workshare Protect Client
- Workshare PDF Converter Version 5.0.159

To install Workshare Protect:

1. Double-click **WorkshareProtect-9800.XXX.exe** (where XXX is the build number).The Workshare Installer is displayed.



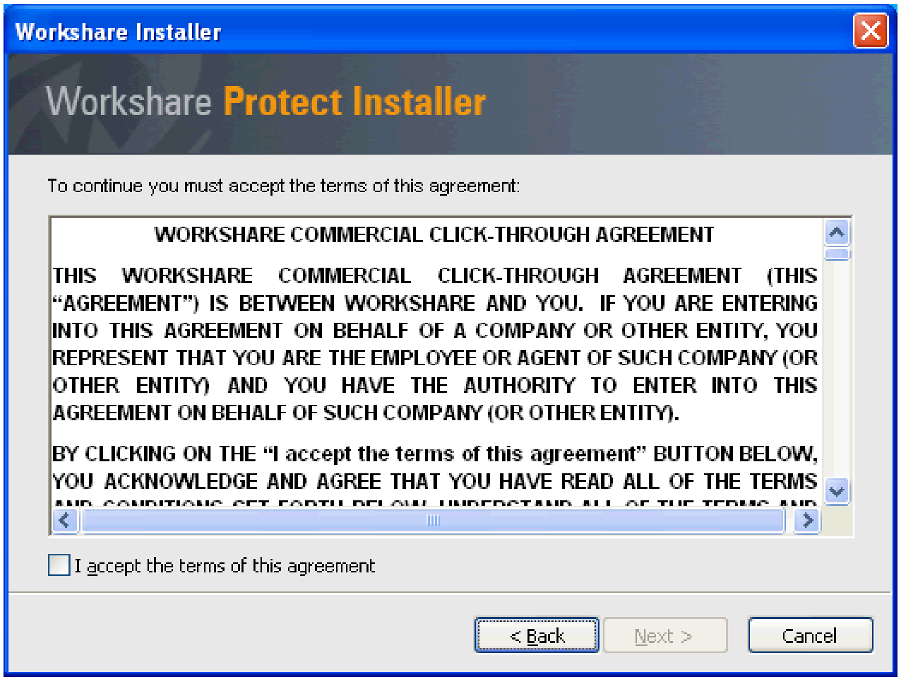
Workshare Installer

Welcome to the Workshare Installer

This is the Workshare Installation Wizard. It is strongly recommended that you exit all Windows programs before running this setup program.

Click 'Next' to continue.

2. Click **Next.** The License Agreement screen is displayed.



Workshare Installer

Workshare Protect Installer

To continue you must accept the terms of this agreement:

WORKSHARE COMMERCIAL CLICK-THROUGH AGREEMENT

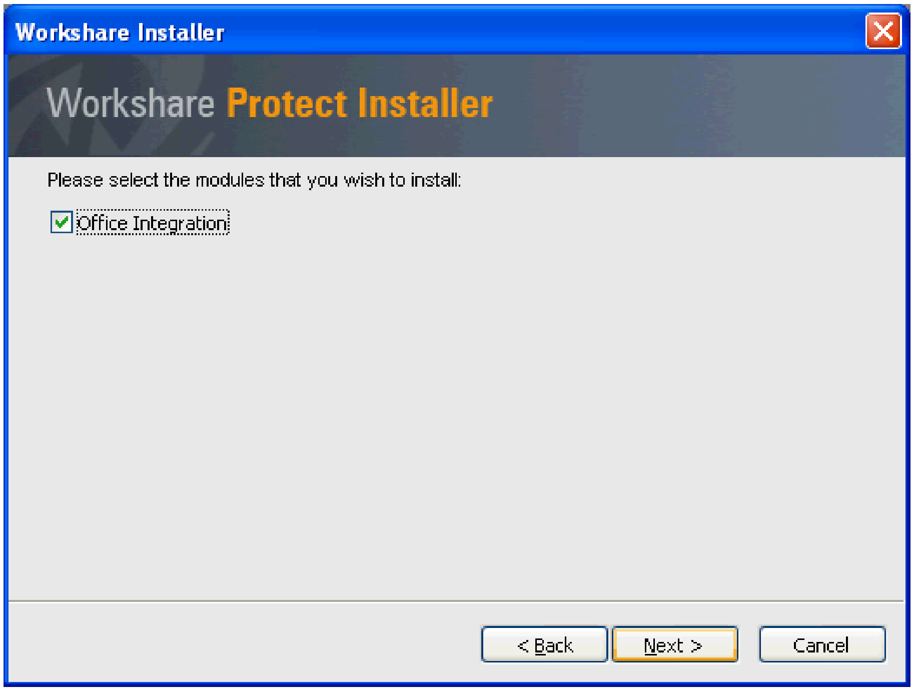
THIS WORKSHARE COMMERCIAL CLICK-THROUGH AGREEMENT (THIS "AGREEMENT") IS BETWEEN WORKSHARE AND YOU. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER ENTITY, YOU REPRESENT THAT YOU ARE THE EMPLOYEE OR AGENT OF SUCH COMPANY (OR OTHER ENTITY) AND YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF SUCH COMPANY (OR OTHER ENTITY).

BY CLICKING ON THE "I accept the terms of this agreement" BUTTON BELOW, YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE READ ALL OF THE TERMS

□ I accept the terms of this agreement

3. Read the agreement and select the **I accept the terms of this agreement** checkbox.

4. Click **Next**.



Workshare Installer

Workshare Protect Installer

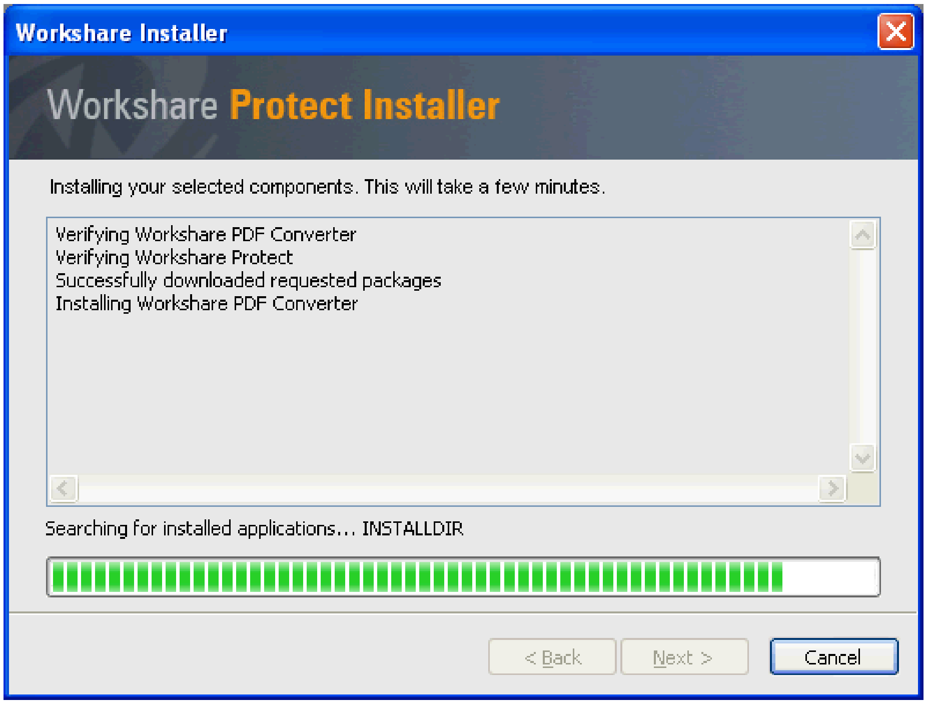
Please select the modules that you wish to install:

☑ Office Integration

5. Select the **Office Integration** checkbox to integrate Workshare Protect within Microsoft Office.

6. Click **Next**. Workshare Protect creates the necessary folders and copy files.

   The installation process may take a few minutes. A progress bar indicates the progress of the installation.



Workshare Installer

Workshare Protect Installer

Installing your selected components. This will take a few minutes.

```
Verifying Workshare PDF Converter
Verifying Workshare Protect
Successfully downloaded requested packages
Installing Workshare PDF Converter
```

Searching for installed applications... INSTALLDIR

7. After this process is completed, click **Finish**. This completes the installation of Workshare Protect. You are now able to start using Workshare Protect. For a full description of the Workshare Protect functionality, refer to the *Workshare Protect User Guide.*

Note: *Ensure that the system user has write access to the policy sets folder - Documents and Settings/All Users/Application Data/Workshare/Protect Enterprise/PolicySets.*

If required, you can now configure Workshare Protect (described in *Chapter 3: Configuration*) or deploy Workshare Protect across your network (described in *Chapter 5: Network Deployment*).

Uninstalling Workshare Protect

Workshare PDF Converter and Workshare Protect should be uninstalled using the **Add or Remove Programs** option in the Control Panel. Uninstalling Workshare PDF Converter and Workshare Protect will uninstall all the Workshare elements installed during the installation process.

Note: *The uninstall process will not uninstall any prerequisites installed.*

Licensing Workshare Protect

This section describes how to license Workshare Protect using a license file or an authorization code. It also describes how to renew a term license.

Licensing Using License Files

A license file is a file with a LIC extension. You can license Workshare Protect using the license file in either of the following ways:

- Copy the license file into the **Modules** folder of the Workshare Protect installation directory on a Workshare Protect workstation, for example, using copy/paste functions or a login script.
- Run the Workshare Configuration Assistant from a command line (described in *Re-Running the WCA*, page 18) and specify the LICFILE parameter.

Licensing Using Authorization Codes

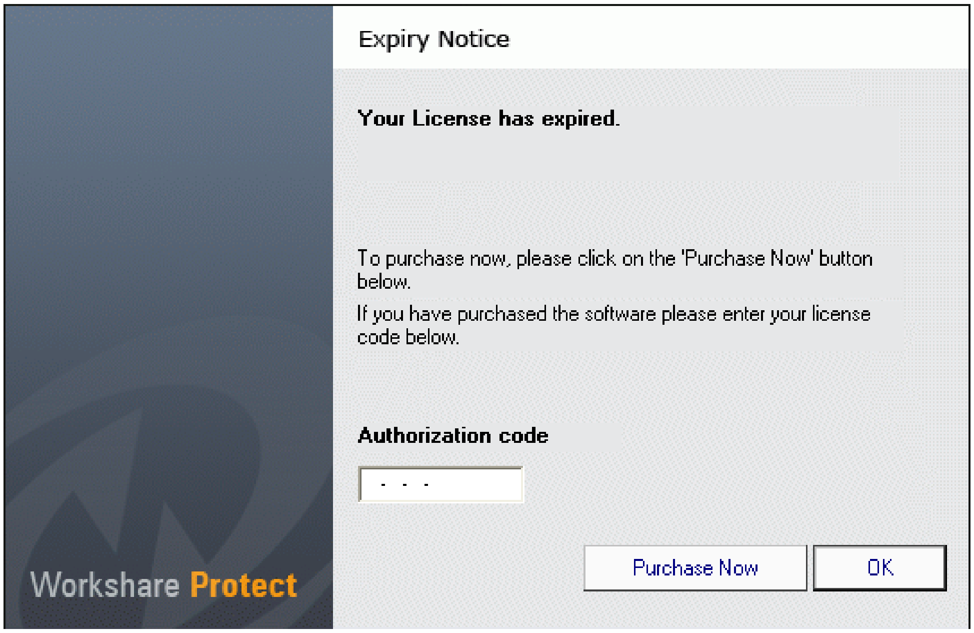
License authorization codes consist of 12 numeric characters broken down into four groups of three, which are split by a dash or '-', for example '012-345-678-910'. Typically, an organization would use one authorization code to license all its users.

You specify the authorization code after installation upon launch of a Microsoft Office application. You can also license Workshare Protect using the authorization code in either of the following ways:

- From the Workshare Configuration Manager, page **Error! Bookmark not defined.**
- Using WmLicGen.exe, page **Error! Bookmark not defined.**

To license Workshare Protect:

1. After installation, launch a Microsoft Office application, for example, Microsoft Word. A reminder screen is displayed, such as the following:



Expiry Notice

Your License has expired.

To purchase now, please click on the 'Purchase Now' button below.

If you have purchased the software please enter your license code below.

Authorization code

2. Enter your authorization code.

In order for license authorization codes to be validated, each client workstation requires an Internet connection. If the user is connecting to the Internet using a proxy server, Workshare Protect will use the proxy server settings from Internet Explorer by default. In addition, it is possible to manually specify the proxy server details if they are not set in Internet Explorer. When a license authorization code is submitted, it is validated by the Workshare Licensing Authorization Server and a license is written to the **Modules** folder of the Workshare Protect installation directory.

> ***Note:*** *The workstation name is recorded on the Workshare Licensing Authorization Server. No other details are recorded.*

It is possible to check connectivity to the Workshare Licensing Authorization Server in two ways:

- In an Internet browser session, enter http://las.workshare.com/CheckConnection in the address line. (Note that the text is case sensitive.) If the connection is successful, the message "You have successfully contacted the Workshare Licensing Authorization Server for external clients (Port 80)" is received.
- From the command line, ping the Workshare Licensing Authorization Server. Enter **"ping las.workshare.com"**. If the connection is successful, a reply is received from the Workshare Licensing Authorization Server.

Once the license is validated, Workshare Protect will create a license file (with a LIC extension) and place it in the **Modules** folder of the Workshare Protect installation directory. In order for Workshare Protect to create a valid license file, the logged on user requires read/write access to the **Modules** folder.

Licensing from the Workshare Configuration Manager

If you are licensing Workshare Protect after installation and you are using an authorization code, you can license Workshare Protect using the Workshare Configuration Manager.

To license Workshare Protect from the Workshare Configuration Manager:

1. From the *Workshare* menu in Microsoft Word, select **Options** (MS Office 2003/XP) or click **Options** in the *Workshare* tab, **Options** group (MS Office 2007). The Options page is displayed in the Workshare Panel.
2. Click **Workshare Application Configuration**. The Workshare Application Configuration Manager is displayed.
3. Select the **Registration** category in the left pane.
4. Click **Get License** in the right pane. The *License Authorization Code* dialog is displayed.
5. Enter your authorization code and click **OK**.
6. Click **OK** in the Workshare Application Configuration Manager.

Licensing Workshare Protect Using WmLicGen.exe

If you are licensing Workshare Protect after installation and you are using an authorization code, you can license Workshare Protect using a command line utility called WmLicGen.exe.

WmLicGen.exe is located in the **Modules** folder of the Workshare Protect installation directory. This executable can be run individually on each workstation or can be deployed to run on multiple workstations, for example, as part of login script.

To license Workshare Protect using the WmLicGen.exe method, the following syntax should be used:

```
WmLicGen.exe /GET XXX-XXX-XXX-XXX
```

Where XXX-XXX-XXX-XXX is your authorization code.

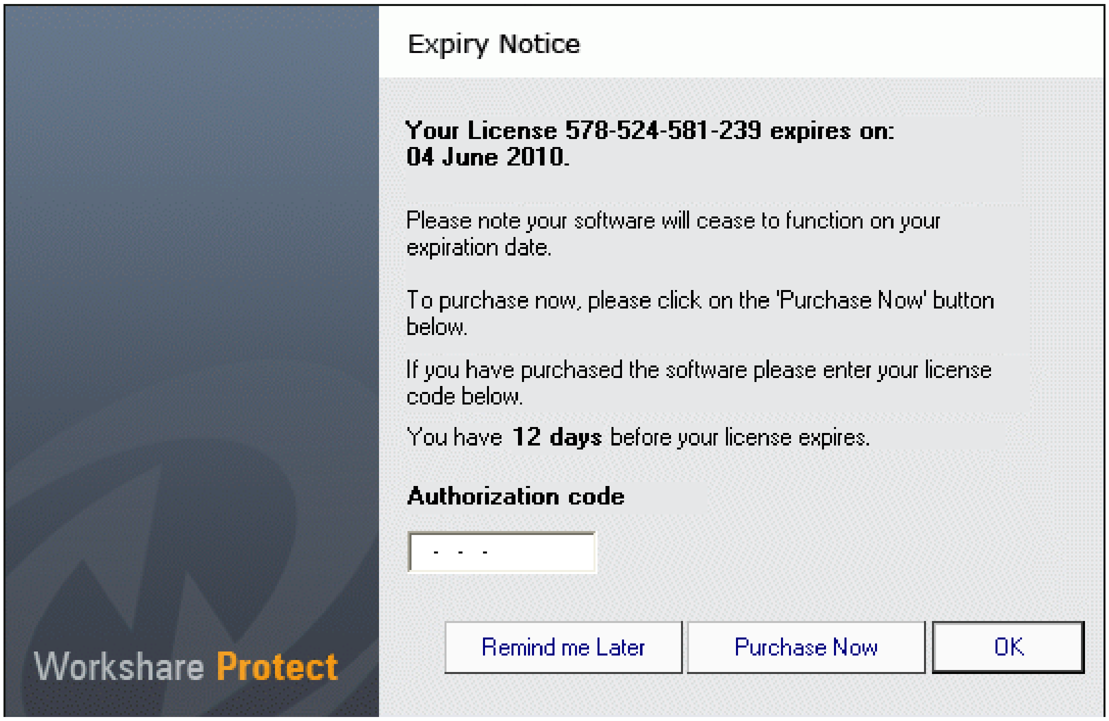
The switches available are as follows:

Switch	Value
No switches	Lists all licenses on system.
?	Displays help.
Get <Auth Code>	Gets the license specified by Auth Code.
Release <Auth Code>	Releases the license specified by Auth Code.
Renew <Auth Code>	Renews the license specified by Auth Code.
Release_All	Releases all licenses with authorization codes.
Renew_All	Renews all licenses with authorization codes.
PORT=X	Specifies the proxy server port number for HTTP traffic (where X is the port number).
ADDRESS=X	Specifies the proxy server address (where X is the name or IP address of the proxy server).

Note: *When working with a proxy server, you must specify both the PORT and ADDRESS switches.*

Renewing a Subscription License

One month before your subscription license expires, you can choose to receive a popup notice on a daily basis.



Expiry Notice

Your License 578-524-581-239 expires on:
04 June 2010.

Please note your software will cease to function on your expiration date.

To purchase now, please click on the 'Purchase Now' button below.

If you have purchased the software please enter your license code below.

You have **12 days** before your license expires.

Authorization code

Proceed in any of the following ways:

- Enter your new or renewed authorization code and click **OK**. Your license is updated and the Expiry Notice is not displayed again.
- Click **OK**. The Expiry Notice will be displayed again on the following day.
- Click **Remind me Later**. The Expiry Notice will be displayed again in 7 days and every 7 days until 7 days before the expiration date when it will be displayed on a daily basis.
- Click **Purchase Now**. You are directed to the Workshare website where you can purchase a new license.

Turning Expiry Notice On/Off

You can prevent the Expiry Notice from displaying on a machine if you do not want users to view the popup. It is recommended that Administrator machines do display the popup to alert for expiring licenses. In the Registry, browse to HKEY_LOCAL_MACHINE\Software\Workshare\Framework\Settings and set the **ShowExpiryReminder** key to **0** to disable the Expiry Notice or **1** to enable the Expiry Notice.

> ***Note:*** *By default, when there is no DMS integration and the install is not silent, this key is set to* ***1*** *and the Expiry Notice is displayed. When the installation includes a DMS integration and/or is Silent, the key is set to* ***0*** *and the Expiry Notice is not displayed.*

Purchasing New Licenses

Visit the Workshare website for ways to purchase a new license. If you have a license (LIC) file, relicense Workshare Protect using the methods described in *Licensing Using License Files*, page 25. You will need to replace any existing license files with the updated one. If you purchase an authorization code (you may be given a new code or advised that your existing code has been updated to reflect the new subscription period), relicense Workshare Protect by entering the code into the Expiry Notice dialog or by using WmLicGen to release and get a license (described in *Licensing Workshare Protect Using WmLicGen.exe*, page 27) or by using the method below.

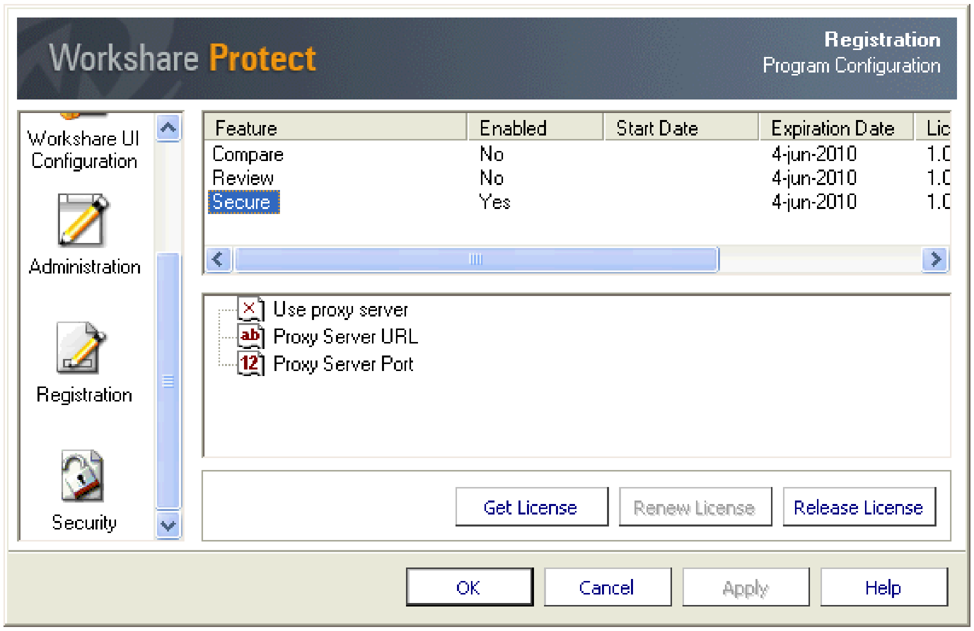
Renewing a License on a Single Machine

This procedure involves releasing the existing expired (or about to expire) license and getting the new license. It MUST be performed even if your authorization code has not changed.

To renew your license:

1. From the *Workshare* menu in Microsoft Word, select **Options** (MS Office 2003/XP) or click **Options** in the *Workshare* tab, **Options** group (MS Office 2007). The Options page is displayed in the Workshare Panel.
2. Click **Workshare Application Configuration**. The Workshare Application Configuration Manager is displayed.
3. Select the **Registration** category in the left pane.

4. In the upper area of the right pane, select **Secure**.

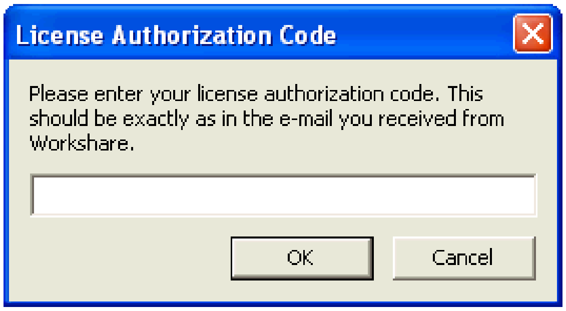


Feature	Enabled	Start Date	Expiration Date	Lic
Compare	No		4-jun-2010	1.0
Review	No		4-jun-2010	1.0
Secure	Yes		4-jun-2010	1.0

☒ Use proxy server
ab Proxy Server URL
12 Proxy Server Port

5. Click **Release License** in the right pane. A message is displayed warning you that the license for all features will be released. Click **Yes** to continue. The license is released and no features are listed in the upper area of the right pane.

6. Click **Get License** in the right pane. The *License Authorization Code* dialog is displayed.



Please enter your license authorization code. This should be exactly as in the e-mail you received from Workshare.

7. Enter your new authorization code and click **OK**.

8. Click **OK** in the Workshare Application Configuration Manager.

Renewing Licenses across your Network

You can re-license Workshare Protect across your network in either of the following ways:

- Replace an existing expired license file in the install directory (by default, Workshare/Modules) with an updated license file that has been created from the new subscription dates. This can be done as part of a login script.
- Run WmLicGen.exe (a command line utility) on the workstations, for example, as part of login script. WmLicGen.exe is installed as part of the installation and must be run from the installation directory. A sample script is provided below which assumes that you have installed to the default location (%ProgramFiles%\Workshare\Modules).

```
c:
cd c:\program files\Workshare\Modules
WmLicGen.exe /renew_all
```

Chapter 3. Configuration

This chapter describes how to use the Workshare Configuration Manager to configure Workshare Protect. It includes the following sections:

- **Introducing the Workshare Configuration Manager**, below, provides an overview of the Workshare Configuration Manager and how you can use it to customize Workshare Protect behavior to suit your organization's requirements.
- **Accessing the Workshare Configuration Manager**, page 33, describes how to access the Workshare Configuration Manager and its parameters.
- **Creating, Saving and Deploying Configuration Files**, page 35, describes how to save configuration parameters to a configuration file as well as deploy the configuration file to other Workshare Protect workstations.
- **Creating, Saving and Deploying Policy Sets**, page 37, describes how to save policy sets and distribute them to other Workshare Protect workstations.
- **Workshare Protect Configuration Parameters**, page 37, provides a detailed description of all the Workshare Protect configuration parameters.

Introducing the Workshare Configuration Manager

The Workshare Configuration Manager enables you to configure Workshare Protect and the way it behaves. Workshare Protect configuration is separated into application configuration (which covers areas such as UI appearance and comparison functionality) and policy configuration (which covers the policy applied by Workshare Protect when determining content risk).

Application Configuration

When Workshare Protect is installed (without a specified configuration file), it includes default configuration settings in the configuration XML files called **Settings.xml** and **Options.xml**. These XML files are installed at the following location: Documents and Settings/Default User/Application Data/Workshare/Workshare. When a user logs on, the XML files are copied to the user's local folder as follows: Documents and Settings/[Current User]/Application Data/Workshare/Workshare. A user can change the settings in the XML files using the Workshare Configuration Manager.

You (the administrator) can use the Workshare Configuration Manager to establish a global set of Workshare Protect parameters that can be used to standardize the use of Workshare Protect across your organization. This is achieved by storing all the Workshare Protect settings in a configuration file. This can be called anything as long as it has an .ini extension and is placed in the **Config** folder of the Workshare Protect installation directory on the Workshare Protect workstations. All the Workshare Protect settings are taken from this file.

On launch of Microsoft Word, Workshare Protect reads the INI file and loads the settings into the configuration XML files. Workshare Protect will only read the INI file if it has a later time stamp or it is a new INI file. Thus manual changes made by individual users on their workstations can override the settings in the INI file. For this reason, you are advised to consider password-protecting access to the Workshare Configuration Manager.

***Note:** When Workshare Protect reads the INI file and loads the settings into the configuration XML files, the default policy files (**Professional5.policy** and **Professional5.runtimepolicy**) are also automatically generated (unless the **Disable automatic generation of default policy** parameter is selected in the **Administration** category of the Workshare Application Configuration Manager).*

Policy Configuration

The installation of Workshare Protect installs a default security policy called **Professional5.policy** at the following location: Documents and Settings/All Users/Application Data/Workshare/Workshare/. The same policy can also be found in a user's local folder as follows: Documents and Settings/[current user]/My Documents/My Policies. When a new user logs in, the default policy is copied to their My Policies folder.

Additionally, a copy of this policy is created in a file called **Professional5.runtimepolicy** at the following location: Documents and Settings/All Users/Application Data/Workshare/Protect Enterprise/PolicySets. It is actually the runtimepolicy file that Workshare Protect applies as the policy set.

The **Professional5.policy** and the **Professional5.runtimepolicy** files are automatically regenerated (thereby replacing any existing default policy files) in the following scenarios:

- When a configuration INI file is deployed.
- When re-running the Workshare Configuration Assistant.
- When applying any changes made in the Workshare Policy Configuration Manager.

***Note:** If you do not want the default policy files to be automatically regenerated in these scenarios, ensure the **Disable automatic generation of default policy** parameter (**Administration** category) is selected.*

A user can change the policy set by modifying the parameters in the Workshare Policy Configuration Manager. Any changes made there update the following files: **Options.xml**, **Professional5.policy** (in the user's My Policies folder) and **Professional5.runtimepolicy**.

You can use the Workshare Policy Configuration Manager to establish a global policy set. Workshare Protect detects sensitive information according to the current policy set. Once you have finalized the policy set, you can use a login script to copy the **Options.xml**, and **Professional5.runtimepolicy** to the Workshare Protect workstations.

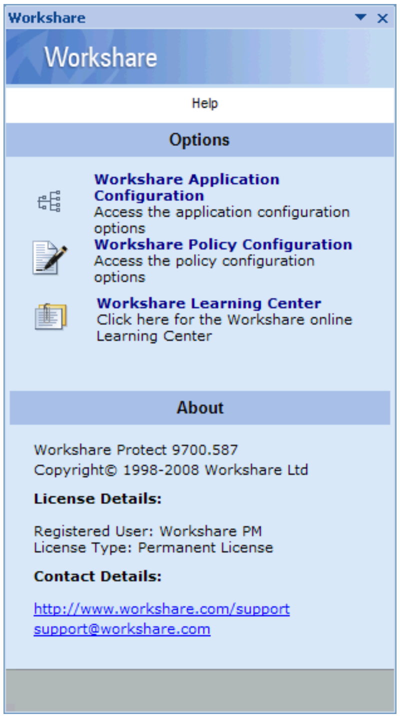
***Note:** Remember that a user can change the default policy set by modifying the parameters in the Workshare Policy Configuration Manager. Thus manual changes made by individual users on their workstations can override the settings in the deployed policy set. For this reason, you should consider password-protecting access to the Workshare Configuration Manager.*

Accessing the Workshare Configuration Manager

The Workshare Configuration Manager is accessed from the Options page of the Workshare Panel. You can limit access to the Workshare Configuration Manager by specifying that a password is required in order to access the Workshare Configuration Manager. (**Password protect access to configuration** parameter in the **Administration** category.)

To access the Workshare Configuration Manager:

1. From the *Workshare* menu in Microsoft Word, select **Options** (MS Office 2003/XP) or click **Options** in the *Workshare* tab, **Options** group (MS Office 2007). The Options page is displayed in the Workshare Panel.



Workshare

Workshare

Help

Options

Workshare Application Configuration
Access the application configuration options

Workshare Policy Configuration
Access the policy configuration options

Workshare Learning Center
Click here for the Workshare online Learning Center

About

Workshare Protect 9700.587
Copyright© 1998-2008 Workshare Ltd

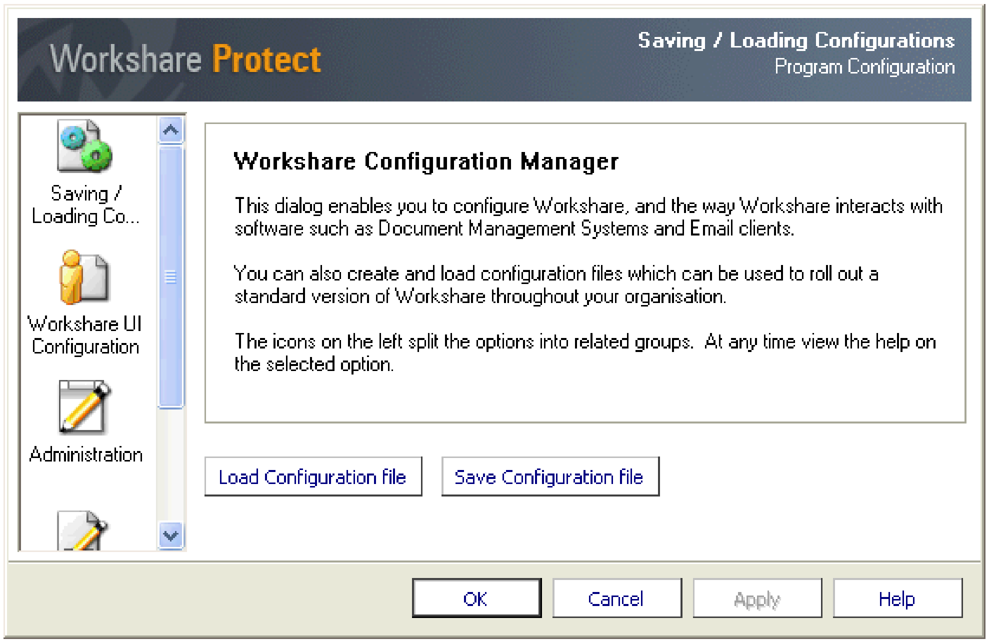
License Details:

Registered User: Workshare PM
License Type: Permanent License

Contact Details:

http://www.workshare.com/support
support@workshare.com

2. Clicking **Workshare Application Configuration** displays the Workshare Application Configuration Manager as follows:



Workshare Protect

Saving / Loading Configurations
Program Configuration

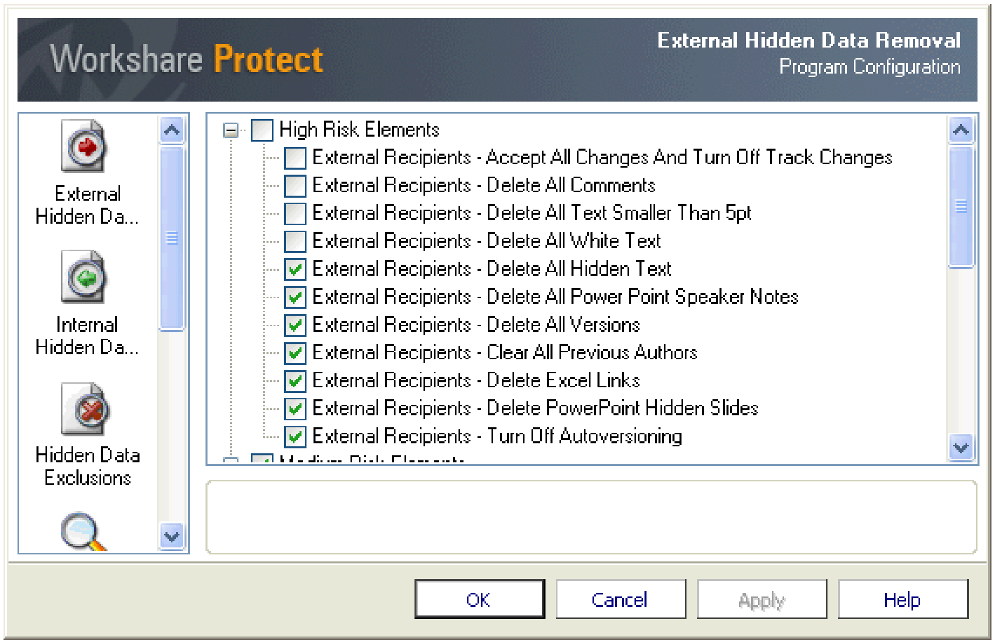
Workshare Configuration Manager

This dialog enables you to configure Workshare, and the way Workshare interacts with software such as Document Management Systems and Email clients.

You can also create and load configuration files which can be used to roll out a standard version of Workshare throughout your organisation.

The icons on the left split the options into related groups. At any time view the help on the selected option.

3. Clicking **Workshare Policy Configuration** displays the Workshare Policy Configuration Manager, as follows:



- □ High Risk Elements
  - □ External Recipients - Accept All Changes And Turn Off Track Changes
  - □ External Recipients - Delete All Comments
  - □ External Recipients - Delete All Text Smaller Than 5pt
  - □ External Recipients - Delete All White Text
  - ☑ External Recipients - Delete All Hidden Text
  - ☑ External Recipients - Delete All Power Point Speaker Notes
  - ☑ External Recipients - Delete All Versions
  - ☑ External Recipients - Clear All Previous Authors
  - ☑ External Recipients - Delete Excel Links
  - ☑ External Recipients - Delete PowerPoint Hidden Slides
  - ☑ External Recipients - Turn Off Autoversioning
- ☑ Medium Risk Elements

The configuration parameters for Workshare Protect are grouped into categories. The categories appear in the left pane of the Workshare Configuration Manager. Selecting a category displays the parameters for that category in the right pane of the Workshare Configuration Manager. The different categories and their parameters are described in *Workshare Protect Configuration Parameters*, page 38.

Creating, Saving and Deploying Configuration Files

Once you have configured Workshare Protect you can save your settings to a configuration (INI) file. This will enable you to restore these settings at some point in the future, or to distribute these settings to other machines without having to manually set the options on each machine.

Saving Configuration Files

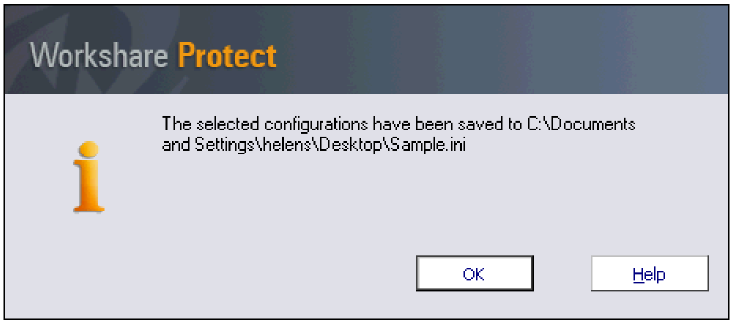
Once you have set the configuration parameters for Workshare Protect in a test installation or on any Workshare Protect workstation, you can save the configuration settings in an INI file and then deploy them to other Workshare Protect workstations. This saves time and enables a consistency within your organization.

To save a configuration file:

1. In the Workshare Application Configuration Manager, configure the Workshare Protect parameters as follows:
   - Click a category in the left pane to display parameters for that category in the right pane.
   - Configure the parameters as required.

   Categories and their parameters are described in *Workshare Protect Configuration Parameters*, page 38.

2. Select **Saving/Loading Configurations** in the left pane.
3. Click **Save Configuration file** in the right pane. A *Save As* dialog is displayed.
4. Name the file as required and navigate to the save location. You can use any name but the file must have an .ini extension.
5. Click **Save**. The following confirmation message is displayed:



The selected configurations have been saved to C:\Documents and Settings\helens\Desktop\Sample.ini

6. Click **OK**. The configuration settings are saved to the specified INI file.

You can now load this INI file onto other individual Workshare Protect workstations or deploy to multiple machines.

Deploying Configuration Files

When deploying a configuration file to Workshare Protect workstations, it must be loaded or copied into the **Config** folder of the Workshare Protect installation directory.

Loading a configuration (INI) file to a Workshare Protect workstation results in the INI file being read and the settings written to the configuration XML files. Additionally the default policy files (**Professional5.policy** and **Professional5.runtimepolicy**) are automatically generated (overriding any existing default policy files).

> ***Note:*** *There must be only* ***one*** *INI file in the* ***Config*** *folder at any time to ensure that only the settings in that INI file are used.*

You can deploy or load configuration files in any of the following ways:

- Use the INIFILE parameter to specify the INI file location when either installing Workshare Protect from the command line or installing Workshare Protect using a deployment tool. Refer to *Chapter 5: Network Deployment*.
- Run the WCA from a command line (described in *Re-Running the WCA*, page 18) and specify the INIFILE parameter.
- Copy the configuration file into the **Modules\Config** folder of the Workshare Protect installation directory on a Workshare Protect workstation, for example, using copy/paste functions or a login script.
- Use the **Load Configuration file** button in the Workshare Application Configuration Manager on an individual Workshare Protect workstation (see procedure on page 37).

Loading Configuration Files from the Workshare Configuration Manager

Using this procedure, the INI file is **NOT** copied to the **Modules\Config** folder of the Workshare Protect installation directory. On launch of Microsoft Word, Workshare Protect reads the INI file and loads the settings into the configuration XML files. You should therefore restart Workshare Protect (by restarting Microsoft Word) after loading a new configuration file to enable the new configuration settings to be applied.

To load a configuration file from the Workshare Configuration Manager:

1. In the Workshare Application Configuration Manager, select **Saving/Loading Configurations** in the left pane.
2. Click **Load Configuration file** in the right pane. The *Open* dialog is displayed.
3. Navigate to the location of the configuration (INI) file that you want to load.
4. Click **Open**.
5. Restart Workshare Protect (by restarting Microsoft Word) to enable the new configuration settings to take place.

Modifying, Saving and Deploying Policy Sets

The default policy set can be edited from the Workshare Policy Configuration Manager. Any changes are saved in the **Professional5.policy** file, the **Professional5.runtimepolicy** file and the **Options.xml** file.

Once you have configured your Workshare Protect policy set, you can distribute the policy set to other machines without having to manually set the policy set on each machine.

Saving Policy Sets

Once you have configured the policy set for Workshare Protect in a test installation or on any Workshare Protect workstation, you can save the policy settings in an INI file and then deploy them to other Workshare Protect workstations. This saves time and enables a consistency within your organization.

To save a policy set:

1. In the Workshare Policy Configuration Manager, configure the Workshare Protect parameters as follows:
   - Click a category in the left pane to display parameters for that category in the right pane.
   - Configure the parameters as required.

   Categories and their parameters are described in *Workshare Protect Configuration Parameters*, page 38.
2. Click **OK**. The policy set is saved and the **Professional5.policy** file, the **Professional5.runtimepolicy** file and the **Options.xml** files are updated.
3. In the Workshare Application Configuration Manager, select **Saving/Loading Configurations** in the left pane.
4. Click **Save Configuration file** in the right pane. A *Save As* dialog is displayed.

5. Name the file as required and navigate to the save location. You can use any name but the file **must** have an .ini extension.

6. Click **Save**. A confirmation message is displayed.

7. Click **OK**. The configuration settings are saved to the specified INI file.

You can now distribute the policy set onto other individual Workshare Protect workstations by loading this INI file onto other individual Workshare Protect workstations or deploying to multiple machines.

Deploying Policy Sets

After working on policies in the Workshare Policy Configuration Manager, you must save the policy settings in a configuration file and then deploy the configuration file to Workshare Protect workstations, by loading or copying it into the **Config** folder of the Workshare Protect installation directory.

Loading a configuration (INI) file to a Workshare Protect workstation results in the INI file being read and the settings written to the configuration XML files. Additionally the default policy files (**Professional5.policy** and **Professional5.runtimepolicy**) are automatically generated (overriding any existing default policy files).

Note: *There must be only* ***one*** *INI file in the* ***Config*** *folder at any time to ensure that only the settings in that INI file are used.*

You can deploy or load configuration files in any of the following ways:

- Use the INIFILE parameter to specify the INI file location when either installing Workshare Protect from the command line or installing Workshare Protect using a deployment tool. Refer to *Chapter 5: Network Deployment*.

- Run the WCA from a command line (described in *Re-Running the WCA*, page 18) and specify the INIFILE parameter.

- Copy the configuration file into the **Modules\Config** folder of the Workshare Protect installation directory on a Workshare Protect workstation, for example, using copy/paste functions or a login script.

Workshare Protect Configuration Parameters

The Application configuration parameters for Workshare Protect are grouped into the following categories:

- Workshare UI Configuration, page 39.

- Administration, page 41.

- Registration, page 42.

- Security, page 43.

The Policy configuration parameters for Workshare Protect are grouped into the following categories:

- External Hidden Data Removal, page 44.

- Internal Hidden Data Removal, page 44.

- Hidden Data Exclusions, page 51.
- Document Alerts, page 54.
- Internal Policy, page 56.
- External Policy, page 58.
- General Policy, page 59.

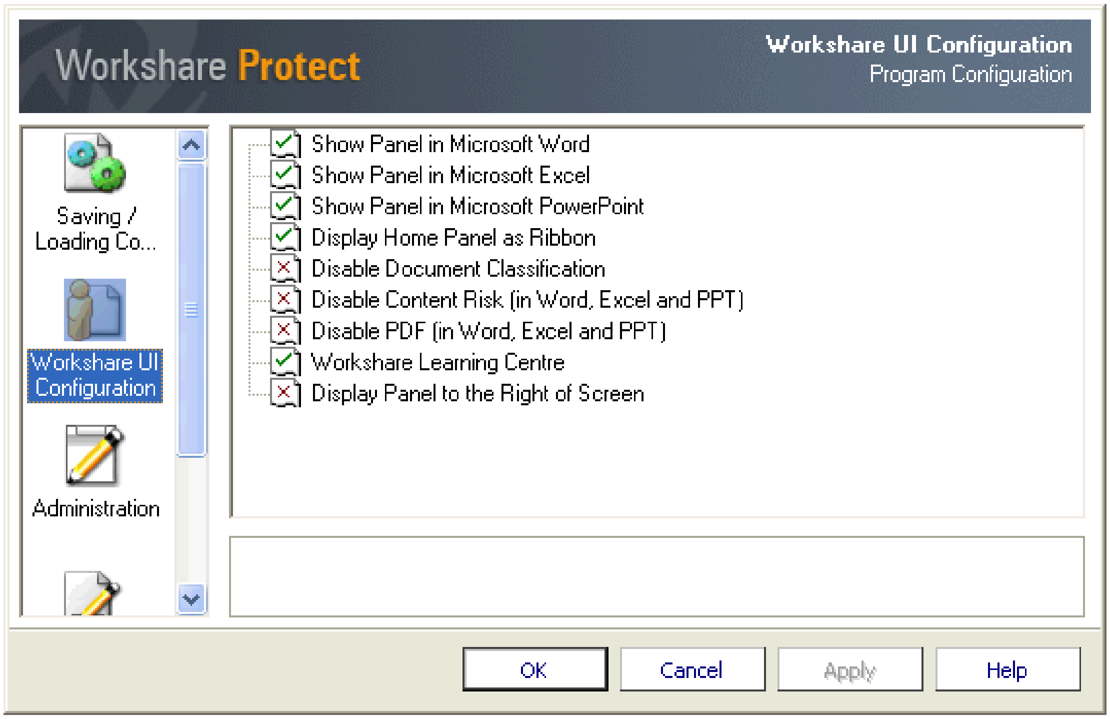
***Note:** You may find that the categories appear in a different order to the one shown here.*

The categories appear in the left pane of the Workshare Configuration Manager. Selecting a category displays the parameters for that category in the right pane of the Workshare Configuration Manager. The different categories and their parameters are described in the following sections.

Workshare UI Configuration

This category is available in the Workshare Application Configuration Manager.

The **Workshare UI Configuration** category includes parameters that enable you to specify how the Workshare user interface is displayed.



☑ Show Panel in Microsoft Word
☑ Show Panel in Microsoft Excel
☑ Show Panel in Microsoft PowerPoint
☑ Display Home Panel as Ribbon
☒ Disable Document Classification
☒ Disable Content Risk (in Word, Excel and PPT)
☒ Disable PDF (in Word, Excel and PPT)
☑ Workshare Learning Centre
☒ Display Panel to the Right of Screen

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

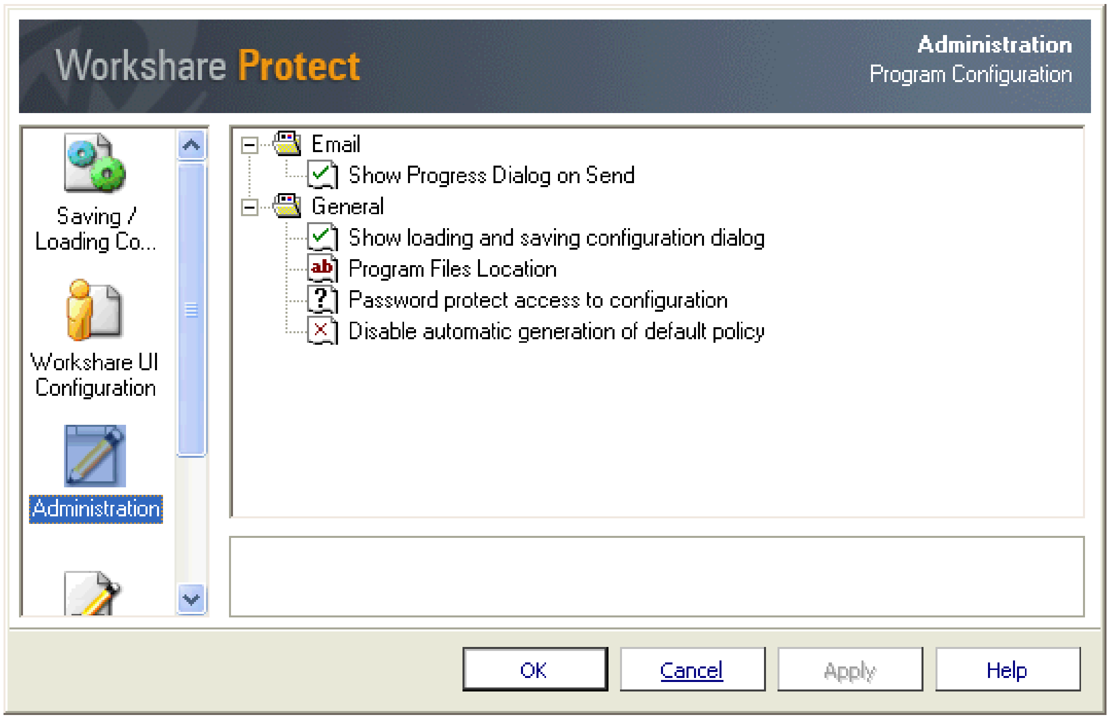
The Workshare UI Configuration parameters are described in the following table:

Parameter	Description
Show Panel in Microsoft Word	If selected, the Workshare Panel is displayed down the left side of the Microsoft Word window.
Show Panel in Microsoft Excel	If selected, the Workshare Panel is displayed down the left side of the Microsoft Excel window.
Show Panel in Microsoft PowerPoint	If selected, the Workshare Panel is displayed down the left side of the Microsoft PowerPoint window.
Display Home Panel as Ribbon	Microsoft Office 2007 only. If selected, the Workshare tab is added to the Ribbon.
Disable Document Classification	If selected, the **Classify** option is disabled in the Workshare menu and the **Classify** option does not appear in the Workshare Panel.
Disable Content Risk (in Word, Excel and PPT)	If selected, the **Show Content Risk** option is disabled in the Workshare menu and the **Content Risk** option does not appear in the Workshare Panel.
Disable PDF (in Word, Excel and PPT)	If selected, the **Convert to PDF** option is disabled in the Workshare menu and the **Convert to PDF** option does not appear in the Workshare Panel.
Replace the Workshare Menu with the Workshare toolbar	Microsoft Office 2003/XP only. If selected, the Workshare menu is removed and the items that appear in the menu are replaced with toolbar icons.
Workshare Learning Center	If selected, the **Workshare Learning Center** option is no longer displayed in the Options page of the Workshare Panel.
Display Panel to the Right of Screen	If selected, the Workshare Panel is displayed down the right side of Microsoft Office windows. When this parameter is changed, you must restart Microsoft Word, Excel or PowerPoint in order for the change to take effect.

Administration

This category is available in the Workshare Application Configuration Manager.

The **Administration** category includes parameters that enable you to specify how Workshare Protect functions in specified situations.



- Email
  - ☑ Show Progress Dialog on Send
- General
  - ☑ Show loading and saving configuration dialog
  - ab Program Files Location
  - ? Password protect access to configuration
  - ☒ Disable automatic generation of default policy

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The Administration parameters are further divided into sub-categories and are described in the following table:

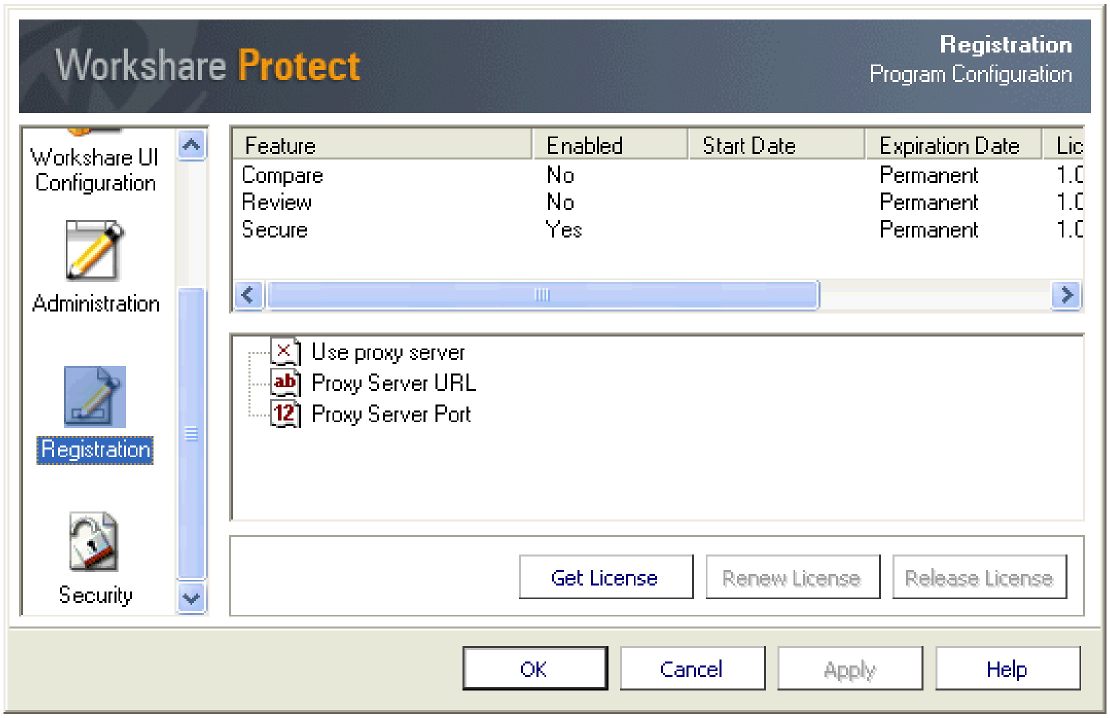
Parameter	Description
EMAIL	
Show Progress Dialog on Send	If selected, a progress bar appears when cleaning and sending an email. This progress bar appears after a number of seconds when the **Show options when sending email externally** (External Policy category) and **Show options when sending mail internally** (Internal Policy category) parameters are not selected. This parameter is selected by default.
GENERAL	
Show loading and saving configuration dialog	If selected, the loading and saving configuration options in the Workshare Configuration Manager are available to the user.
Program Files Location	Displays (read-only) the directory in which Workshare Protect is installed.
Password protect access to configuration	The password required for accessing the Workshare Configuration Manager. For extra security, you can password-protect the Workshare Configuration Manager.

Parameter	Description
Disable automatic generation of default policy	If selected, the default policy files are no longer automatically generated when a configuration INI file is deployed, when re-running the Workshare Configuration Assistant or when applying any changes made in the Workshare Policy Configuration Manager. This is useful if you want to deploy a personalized company policy and you do not want the default policy to exist as well.

Registration

This category is available in the Workshare Application Configuration Manager.

The **Registration** category includes parameters that enable you to specify proxy server settings and update and release licenses.



Feature	Enabled	Start Date	Expiration Date	Lic
Compare	No		Permanent	1.0
Review	No		Permanent	1.0
Secure	Yes		Permanent	1.0

- ☒ Use proxy server
- Proxy Server URL
- Proxy Server Port

In the upper area of the right pane, license information is displayed. The parameters are displayed in the middle area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The Registration parameters are described in the following table:

Parameter	Description
Use proxy server	If selected, enables the use of an Internet proxy server to connect to the Workshare Licensing Authorization Server.
Proxy Server URL	The URL of an Internet proxy server (if used).
Proxy Server Port	The port of an Internet proxy server (if used).

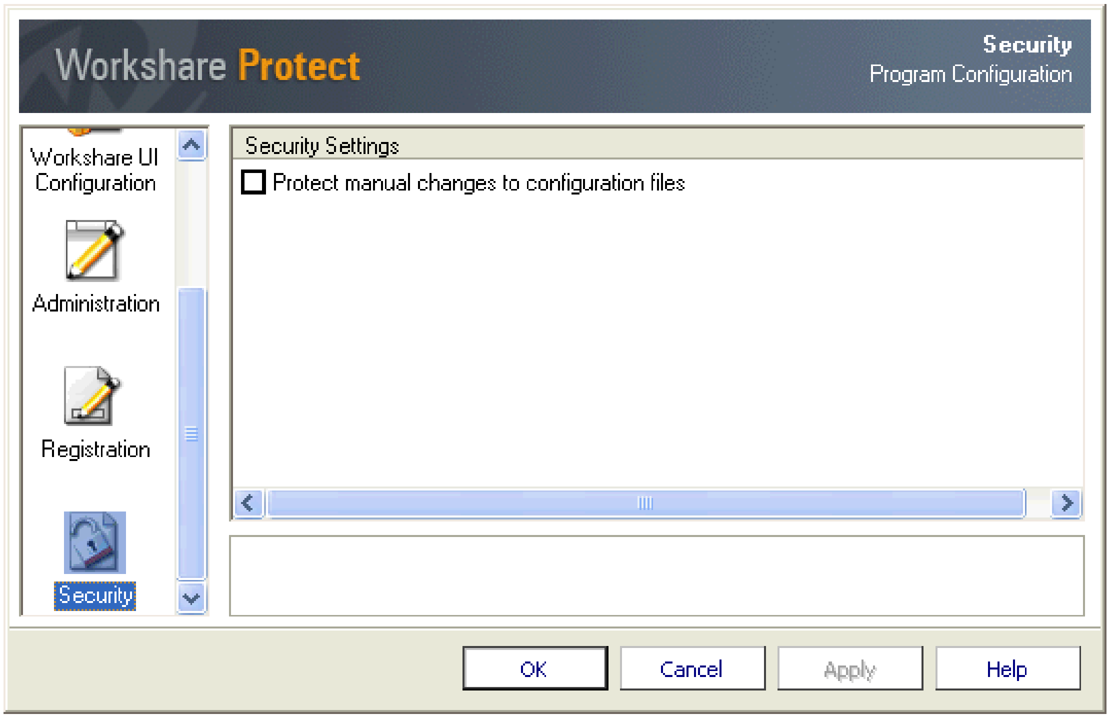
The buttons in the right pane are as follows:

Parameter	Description
Get License	Enables you to enter a Workshare Protect license authorization code. This is then validated by the Workshare Licensing Authorization Server via the Internet.
Renew License	This feature is disabled.
Release License	Removes the license from this workstation.

Security

This category is available in the Workshare Application Configuration Manager.

The **Security** category includes one parameter that enables you to protect the configuration from a user manually changing the configuration files.

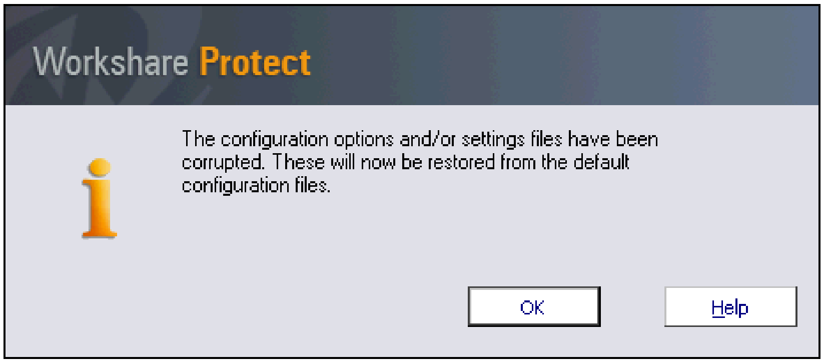


Security Settings

□ Protect manual changes to configuration files

The XML configuration files (**Settings.xml** and **Options.xml**) store the settings and options that have been configured from the Configuration Manager. These files are stored in C:\Documents and Settings\{USER}\Application Data\Workshare\Workshare\ (where {USER} represents "All Users", "Default User" and the username of the user currently logged on).

If the **Protect manual changes to configuration files** parameter is selected and a user manually changes one of the XML configuration files, the following message is displayed when the user opens Microsoft Office.



The configuration options and/or settings files have been corrupted. These will now be restored from the default configuration files.

When you click **OK**, Workshare Protect will restore the default configuration files and therefore override any changes made by the user manually changing the configuration files.

Internal/External Hidden Data Removal

This category is available in the Workshare Policy Configuration Manager.

The **Internal Hidden Data Removal** and **External Hidden Data Removal** categories include parameters that enable you to specify which hidden data should be removed from email attachments. There are two Hidden Data Removal categories: **External Hidden Data Removal** that includes parameters for external recipients, and **Internal Hidden Data Removal** that includes parameters for internal recipients. The parameters in both categories are the same but one set applies to internal recipients and the other applies to external recipients. Different settings can be set for each. You may want to remove all hidden data when sending emails externally, but only remove track changes and hidden text when emailing internally.

Recipient Checking

When you send an email, Workshare Protect takes each recipient in the **To**, **Cc** and **Bcc** fields, and looks them up in the configured address book(s). Usually this is the contacts list or local address book (on your machine) and the global address book (on the server).

> ***Note:*** *To ensure that Workshare Protect can integrate with the local and global address books when users are offline, please refer to* Chapter 4: Integration*.*

For each address there are three possible outcomes:

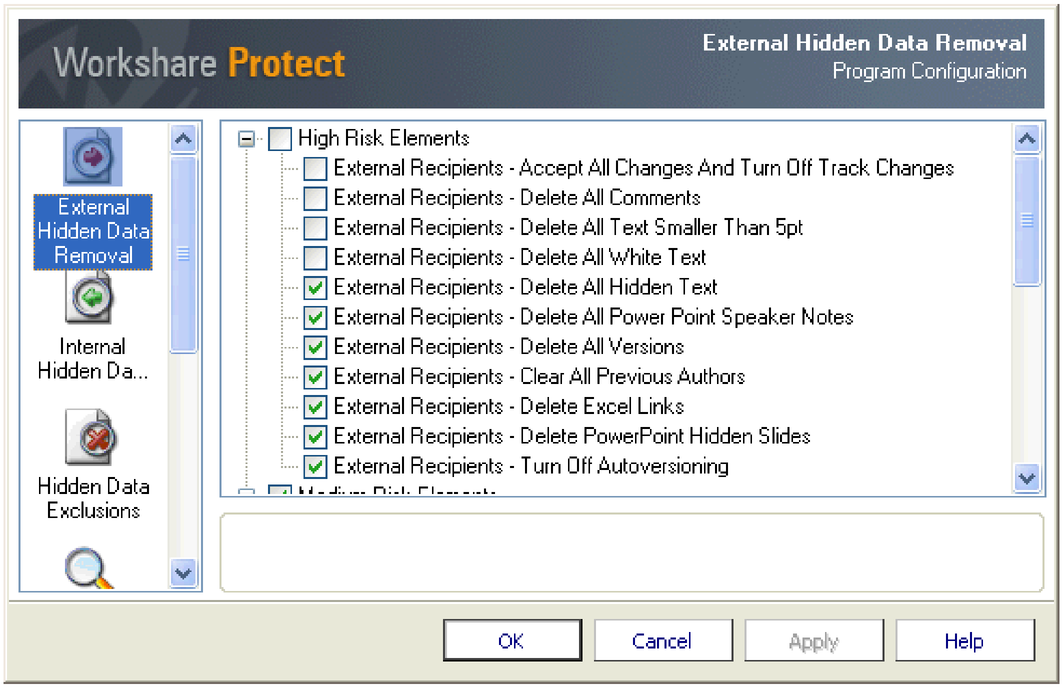
- The address does not exist in any address book. This is then processed as external.
- The address is a distribution list. In this case, the address of each member of the distribution list is checked.

- The address exists in one of the address books. If so, Workshare Protect does a further check that checks the type of address. Either it will be an Exchange\Notes address (meaning the address exists on the email server), or it will be an SMTP address (meaning the email will be routed via the Internet). If it is a server address, it is processed as internal. If it is an SMTP address, it is processed as external.

When deciding which hidden data options to apply, each recipient is checked. If an external recipient is found, external hidden data settings are applied. Only if all recipients are internal, are internal hidden data settings applied.

***Note**: Using the **Treat the following addresses as internal** parameter (Internal Policy category), you can specify external email addresses that you would like to be treated as internal for the purpose of Workshare Protect applying policies.*

The External Hidden Data Removal parameters are as follows:



- ☐ High Risk Elements
  - ☐ External Recipients - Accept All Changes And Turn Off Track Changes
  - ☐ External Recipients - Delete All Comments
  - ☐ External Recipients - Delete All Text Smaller Than 5pt
  - ☐ External Recipients - Delete All White Text
  - ☑ External Recipients - Delete All Hidden Text
  - ☑ External Recipients - Delete All Power Point Speaker Notes
  - ☑ External Recipients - Delete All Versions
  - ☑ External Recipients - Clear All Previous Authors
  - ☑ External Recipients - Delete Excel Links
  - ☑ External Recipients - Delete PowerPoint Hidden Slides
  - ☑ External Recipients - Turn Off Autoversioning

The parameters are displayed in the right pane and are divided into High, Medium and Low risk data. You select a parameter by selecting the checkbox to the left of the parameter. Selecting the checkbox to the left of, for example, **High Risk Elements** selects all the hidden data parameters in that category.

***Tip!** You can select a category (for example, **Medium Risk Elements**) and then deselect one or two hidden data parameters within that category as required.*

You can also select whether to allow the user to override these settings. When you select a parameter, an **Allow users to override** checkbox is displayed in the lower right pane. If you want users to be able to override your setting for the selected parameter, select this checkbox. Otherwise, the user will be unable to change the setting. This checkbox is selected by default, therefore, you must uncheck the checkbox to lock your settings.

*Tip! To lock all settings, deselect the **Allow users to change advanced hidden data options when sending** parameter in the **General Policy** category. Refer to* General Policy*, page 59, for more information.*

The Hidden Data Removal parameters (both Internal and External) are described in the following table:

Parameter	Description
HIGH RISK ELEMENTS:	
Accept All Changes And Turn Off Track Changes	Microsoft Word and Excel. If selected, 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. By default this parameter is not selected.
Delete All Comments	Microsoft Word, Excel and PowerPoint. If selected, removes any comments embedded in the document. By default this parameter is not selected. To display comments: In MS Office 2003/XP, open the Reviewing toolbar and from the **Show** dropdown list, select **Comments.** In MS Office 2007, click the **Review** tab and from the **Balloons** dropdown list (**Tracking** group), select **Show Only Comments and Formatting in Balloons**.
Delete All Text Smaller Than 5pt	Microsoft Word only. If selected, removes all text that has been formatted with a font size less that 5pt (i.e. 4pt and less). By default this parameter is not selected. To view small text: In MS Word 2003/XP, from the *View* menu select **Zoom** and specify a percentage greater than 100%. In MS Word 2007, click the **View** tab, select **Zoom** and specify a percentage greater than 100%.
Delete All White Text	Microsoft Word only. If selected, removes all text that has been formatted with a font color of white and has no background color. By default this parameter is not selected. To view white text: In MS Word 2003/XP, from the *Tools* menu, select **Options**. Select the **General** tab and in the **General options** section, select the **Blue background, white text** checkbox. In MS Word 2007, click the **Page Layout** tab and select a color from the **Page Color** dropdown list (**Page Background** group).
Delete All Hidden Text	Microsoft Word only. If selected, removes all text that has been formatted as hidden. To view hidden text: In MS Word 2003/XP, from the *Tools* menu, select **Options**. Select the **View** tab and in the **Formatting marks** section, select the **Hidden Text** checkbox. In MS Word 2007, click the Office Button, select **Word Options** and then select **Display**. Select the **Hidden Text** checkbox.

Parameter	Description
Delete all PowerPoint Speaker Notes	Microsoft PowerPoint only. If selected, 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.
Delete All Versions	Microsoft Word only. If selected, 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. Document versions are not supported in MS Office 2007. To view versions: From the *File* menu, select **Versions**.
Clear All Previous Authors	Microsoft Word only. If selected, 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.
Delete Excel Links	Microsoft Excel only. If selected, converts external links in Microsoft Excel files to text. The following are examples of external links: 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.
Delete PowerPoint Hidden Slides	Microsoft PowerPoint only. If selected, 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.
Turn Off Autoversioning	Microsoft Word only. If selected, 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.

Parameter	Description
MEDIUM RISK ELEMENTS:	
Delete All Custom Properties	Microsoft Word, Excel and PowerPoint. If selected, removes any custom properties that have been added to the document. ***Note:*** *You can prevent certain custom properties from being cleaned, for example, DMS Doc ID Properties, by selecting them in the* ***Hidden Data Exclusions*** *category. Refer to* Hidden Data Exclusions*, page 51.* To view document properties: In MS Office 2003/XP, open the *File* menu and select **Properties**. In MS Office 2007, click the Office Button, select **Prepare** and then select **Properties**. In the Document Information Panel, select **Advanced Properties** from the **Document Properties** dropdown list. In the *Properties* dialog, select the **Custom** tab.
Delete All Document Variables	Microsoft Word only. If selected, deletes all document variables. 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. Variables can be viewed in Microsoft Word in the Visual Basic Editor.
Delete All Macros	Microsoft Word only. If selected, removes VBA macros from the document. This feature is not intended as virus protection, but rather to protect any confidential information, intellectual property or formulas included in the macros. To view macros: In MS Word 2003/XP, open the *Tools* menu and select **Macro** and then **Macros**. In MS Office 2007, click the **View** tab and select **Macros** and then **View Macros**.
Delete Routing Slip	Microsoft Word and Excel. If selected, 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. Routing slips are not supported in MS Office 2007. To view routing slip entries: From the *File* menu, select **Send To** and then **Routing Recipient**. To view envelope information: From the *File* menu, select **Send To** and then **Mail Recipient**.

Parameter	Description
Clear All Document Reviewers	Microsoft Word only. If selected, 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. To see reviewers list: In MS Word 2003/XP, open the Reviewing toolbar and from the **Show** dropdown list, select **Reviewers**. In MS Office 2007, click the **Review** tab and from the **Show Markup** dropdown list (**Tracking** group), select **Reviewers**. ***Note:*** *Clearing reviewers but not track changes, may be useful if you are collaborating on a document with an external party who uses track changes. You can retain the actual track changes made in the document, but you can remove confidential information about the author within your organization that made the change.*
Delete Ink Annotations (Lightspeed Clean Only)	Microsoft Word, Excel and PowerPoint. If selected, removes ink annotations made in Tablet PC. Ink annotations are only removed by a Lightspeed clean.
LOW RISK ELEMENTS:	
Delete Footnotes	Microsoft Word only. If selected, removes any footnotes or endnotes included in the document. By default this parameter is not selected.
Convert Field Codes To Text	Microsoft Word, Excel and PowerPoint. If selected, 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. ***Note:*** *For Microsoft Excel and PowerPoint, hyperlinks are the only field codes that exist.* 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. ***Note:*** *You can prevent certain field codes from being cleaned, for example, table of contents or page numbers, by selecting them in the Hidden Data Exclusions category. Refer to* Hidden Data Exclusions*, page 51.* To view field codes: In MS Word 2003/XP, open the *Tools* menu and select **Options**. In the **View** tab, select the **Field Codes** checkbox in the **Show** area. In MS Word 2007, click the Office Button, select **Word Options** and then select **Advanced**. Select the **Show field codes instead of their values** checkbox in the **Show document content** area.

Parameter	Description
Reset Document Statistics	Microsoft Word only. If selected, resets all the document statistics - total edit time, revision number, last authors, and file dates. To view statistics: In MS Word 2003/XP, open the *File* menu and select **Properties**. In the *Properties* dialog, select the **Statistics** tab. In MS Word 2007, click the Office Button, select **Prepare** and then select **Properties**. In the Document Information Panel, select **Advanced Properties** from the **Document Properties** dropdown list In the *Properties* dialog, select the **Statistics** tab. ***Note:*** *This information cannot be cleaned from within Microsoft Word.*
Clear All Built-In Properties	Microsoft Word, Excel and PowerPoint. If selected, removes all summary properties - author, category, comments, company, keywords, manager, title, subject, and hyperlink base; and custom properties – text, date and number. To view built-in properties: In MS Office 2003/XP, open the *File* menu and select **Properties**. In the *Properties* dialog, select the **Summary** and **Contents** tabs. In MS Office 2007, click the Office Button, select **Prepare** and then select **Properties**. In the Document Information Panel, select **Advanced Properties** from the **Document Properties** dropdown list. In the *Properties* dialog, select the **Summary** and **Contents** tabs.
Delete All Excel and PowerPoint Headers	Microsoft Excel and PowerPoint. If selected, removes any headers included in the sheet or slide. To view headers and footers: In MS Excel and PowerPoint 2003/XP, open the *View* menu and select **Header and Footer**. In MS Excel and PowerPoint 2007, click the **Insert** tab and select **Header & Footer** (**Text** group).
Delete All Excel and PowerPoint Footers	Microsoft Excel and PowerPoint. If selected, removes any footers included in the sheet or slide. To view headers and footers: In MS Excel and PowerPoint 2003/XP, open the *View* menu and select **Header and Footer**. In MS Excel and PowerPoint 2007, click the **Insert** tab and select **Header & Footer** (**Text** group).
Delete Smart Tags	Microsoft Word only. If selected, removes smart tags from Microsoft Word documents. 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. Smart tags only exist in Microsoft Office XP and later. To manage smart tags: In MS Word XP, open the *Tools* menu and select **AutoCorrect Options**. Select the **Smart Tags** tab. In MS Word 2007, click the Office Button, select **Word Options** and then select **Proofing**. Click the **AutoCorrect Options** button and select the **Smart Tags** tab.

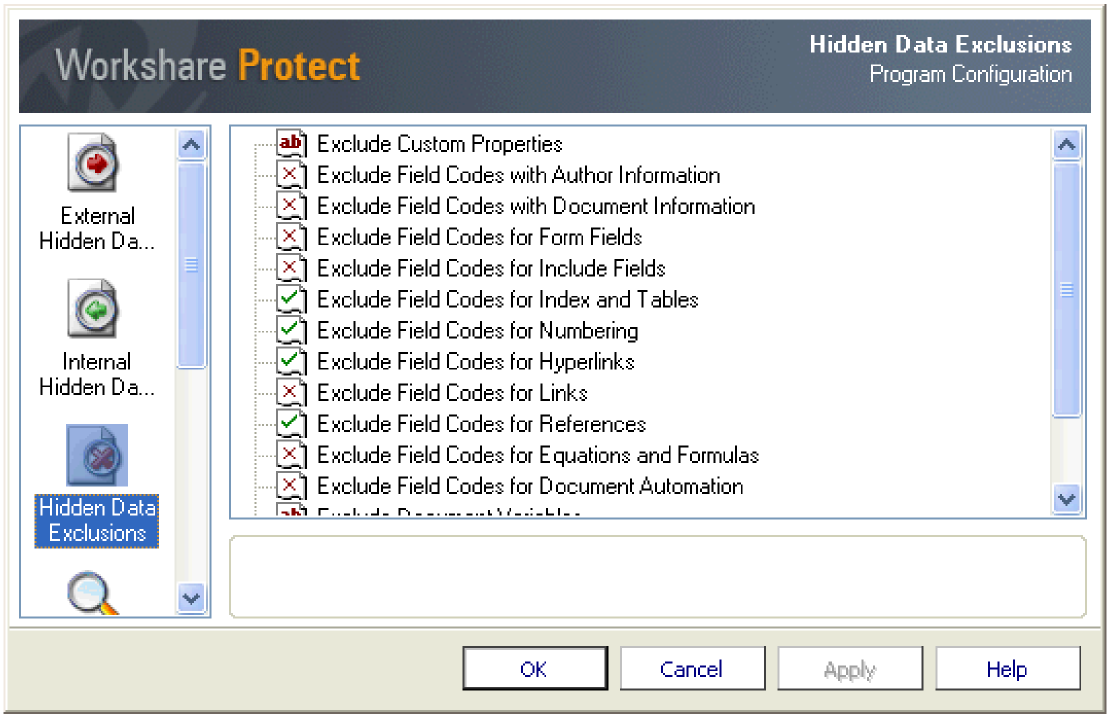
Parameter	Description
Convert Attached Template To Normal	Microsoft Word only. If selected, converts the attached template to normal.dot. Automatic style updating is disabled before the template is removed. Therefore the formatting and styles in your document will not be affected by removing the attached template. To view the attached template: In MS Word 2003/XP, open the *Tools* menu and select **Templates and Add-Ins**. In MS Word 2007, click the Office Button, select **Word Options** and then select **Add-Ins**. From the **Manage** dropdown list, select **Word Add-ins** and click **Go**.

Hidden Data Exclusions

This category is available in the Workshare Policy Configuration Manager.

The **Hidden Data Exclusions** category includes parameters that enable you to exclude certain types of hidden data from being removed when documents are cleaned. The types of hidden data that can be excluded from cleaning are custom properties and field codes. When cleaning, the user can still select to clean custom properties and all custom properties or field codes will be cleaned, except for the ones explicitly excluded here.

> ***Note:*** *When field codes are cleaned, the text is not removed. The field code is simply unlinked so that it is not updated in the future. For example, if you have a table of contents field code. Unlinking it keeps the table of contents in your document, but you are unable to update the table of contents, as it is no longer a field; it is only text.*



- ab Exclude Custom Properties
- ☒ Exclude Field Codes with Author Information
- ☒ Exclude Field Codes with Document Information
- ☒ Exclude Field Codes for Form Fields
- ☒ Exclude Field Codes for Include Fields
- ☑ Exclude Field Codes for Index and Tables
- ☑ Exclude Field Codes for Numbering
- ☑ Exclude Field Codes for Hyperlinks
- ☒ Exclude Field Codes for Links
- ☑ Exclude Field Codes for References
- ☒ Exclude Field Codes for Equations and Formulas
- ☒ Exclude Field Codes for Document Automation
- ab Exclude Document Variables

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The Hidden Data Exclusions parameters are described in the following table:

Parameter	Description
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. If the custom property name includes a space, you must enclose it in quotes. For example, "Matter Id";DocumentName
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. By default, these field codes are not excluded and therefore author information is unlinked during cleaning.
Exclude Field Codes with Document Information	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. If selected, any field codes referencing the document properties or statistics are not cleaned. By default, these field codes are not excluded and therefore document information is unlinked during cleaning.
Exclude Field Codes for Form Fields	These are field codes that are used in forms, for example, dropdown lists and text boxes. If selected, any form field codes are not cleaned. By default, these field codes are not excluded and therefore form fields are unlinked during cleaning.
Exclude Field Codes for Include Fields	These are field codes that include text or pictures from other sources. If selected, any ‘include’ field codes are not cleaned. By default, these field codes are not excluded and therefore ‘include’ fields are unlinked during cleaning.
Exclude Field Codes for Index and Tables	These are field codes related to the Table of Contents, Table of Authorities, Glossary, and Index. If not selected, these tables are unlinked, and can therefore no longer be automatically updated. By default, these field codes are excluded and therefore Tables and Indexes in your document will remain fully functional. ***Note:*** *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.*

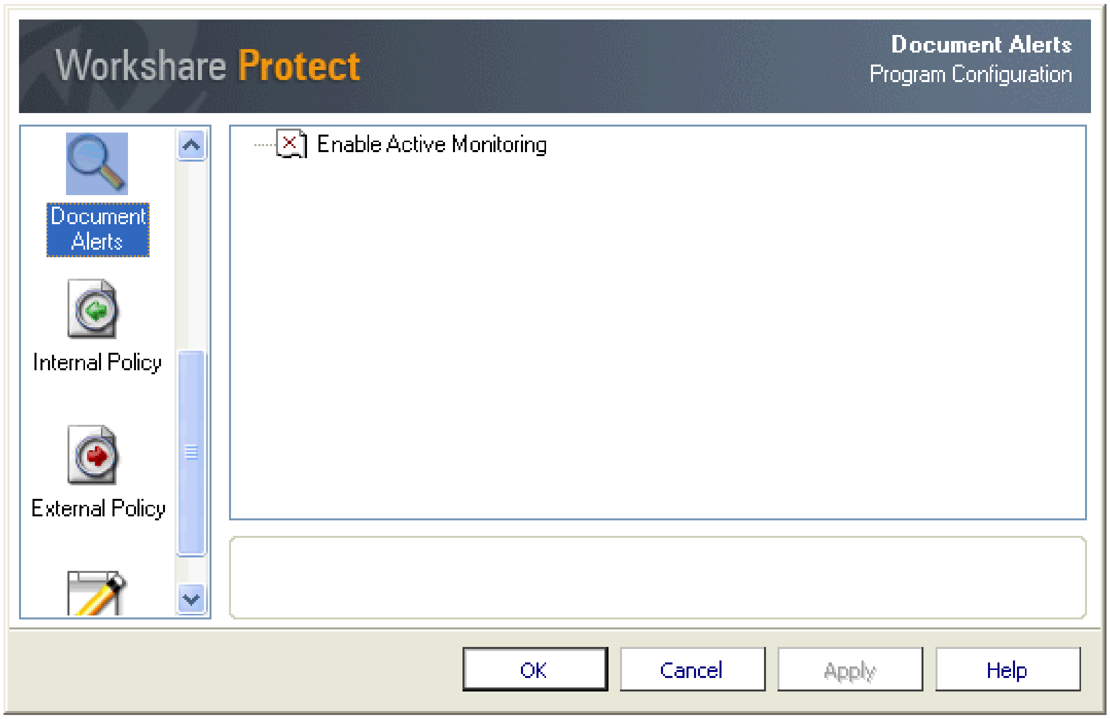
Parameter	Description
Exclude Field Codes for Numbering	These are field codes for numbering within the document, for example, page numbers, list numbers, section numbers. If not selected, these numbers are unlinked and therefore no longer automatically updated. By default, these field codes are excluded and therefore any numbering in your document remains fully functional. ***Note:*** *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.*
Exclude Field Codes for Hyperlinks	These are field codes for hyperlinks. If not selected, hyperlinks are unlinked. The text of the link is still visible but the associated address is removed. By default, these field codes are excluded and therefore hyperlinks in your document remain fully functional.
Exclude Field Codes for Links	These are field codes for linked or imported objects. If selected, the links are not removed and therefore still update from the source. By default, these field codes are not excluded and therefore links are unlinked during cleaning.
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. By default, these field codes are excluded and therefore any references in your document remain fully functional.
Exclude Field Codes for Equations and Formulas	These are field codes for calculations, for example, equations, symbols or formula. If selected, equations remain linked. By default, these field codes are not excluded and therefore any equations are unlinked during cleaning.
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. By default these field codes are not excluded, and therefore document automation features are unlinked during cleaning.
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.

Parameter	Description
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.

Document Alerts

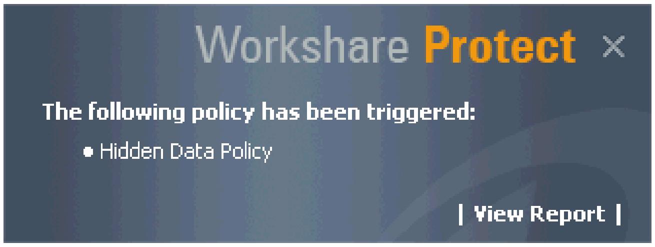
This category is available in the Workshare Policy Configuration Manager.

The **Document Alerts** category includes one parameter that enables you to launch active monitoring of open Microsoft Office documents.



☒ Enable Active Monitoring

If **Enable Active Monitoring** is selected, Workshare Protect checks an open Microsoft Office document as you are working on it to see if it breaches any security policies. If a policy breach is found and the action specified for a policy breach in the security policy is an Active Task Bar action, then a real-time policy alert is displayed to the user. Workshare Protect continuously monitors the active document and alerts the user to any changes in the level of risk contained within the document.



The following policy has been triggered:

- Hidden Data Policy

A real-time policy alert is displayed in the following circumstances:

- When a policy breach occurs for the first time. (A real-time policy alert is not displayed for subsequent breaches of the same policy unless the breach is of a condition with a higher risk level).
- When a document that includes a policy breach is saved.
- When a document that includes a policy breach is opened.

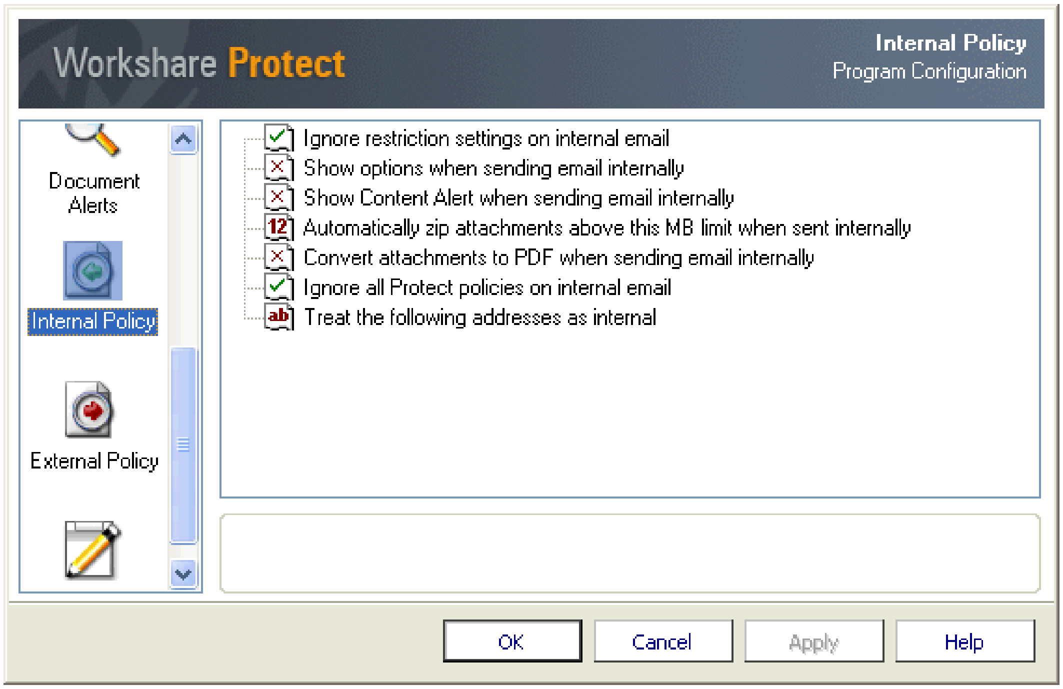
Note: *When Workshare Protect is installed, this parameter is NOT enabled. If you want to activate real-time alerts, you MUST select this parameter and then log off and back on again so the setting is detected and active monitor started.*

Internal Policy

This category is available in the Workshare Policy Configuration Manager.

The **Internal Policy** category includes parameters that enable you to specify the policy to be applied when sending emails to internal recipients.

> ***Note:** When specifying parameters in the **Internal Policy** category, bear in mind that where emails are sent to multiple recipients and at least one is an external recipient, then external policy settings are applied.*



☑ Ignore restriction settings on internal email
☒ Show options when sending email internally
☒ Show Content Alert when sending email internally
12 Automatically zip attachments above this MB limit when sent internally
☒ Convert attachments to PDF when sending email internally
☑ Ignore all Protect policies on internal email
ab Treat the following addresses as internal

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The Internal Policy parameters are described in the following table:

Parameter	Description
Ignore restriction settings on internal email	When this setting is selected, document restriction settings are not checked on attachments to internal emails. This parameter is not selected by default.
Show options when sending email internally	If selected, users will see the *Email Security* dialog with options to convert to PDF or remove hidden data when they send documents to internal users. When this setting is not selected, users will not see the *Email Security* dialog and the email is processed according to the hidden data cleaning and PDF options specified in the configuration. By default, this parameter is not selected so the *Email Security* dialog is not displayed when emailing to internal users.

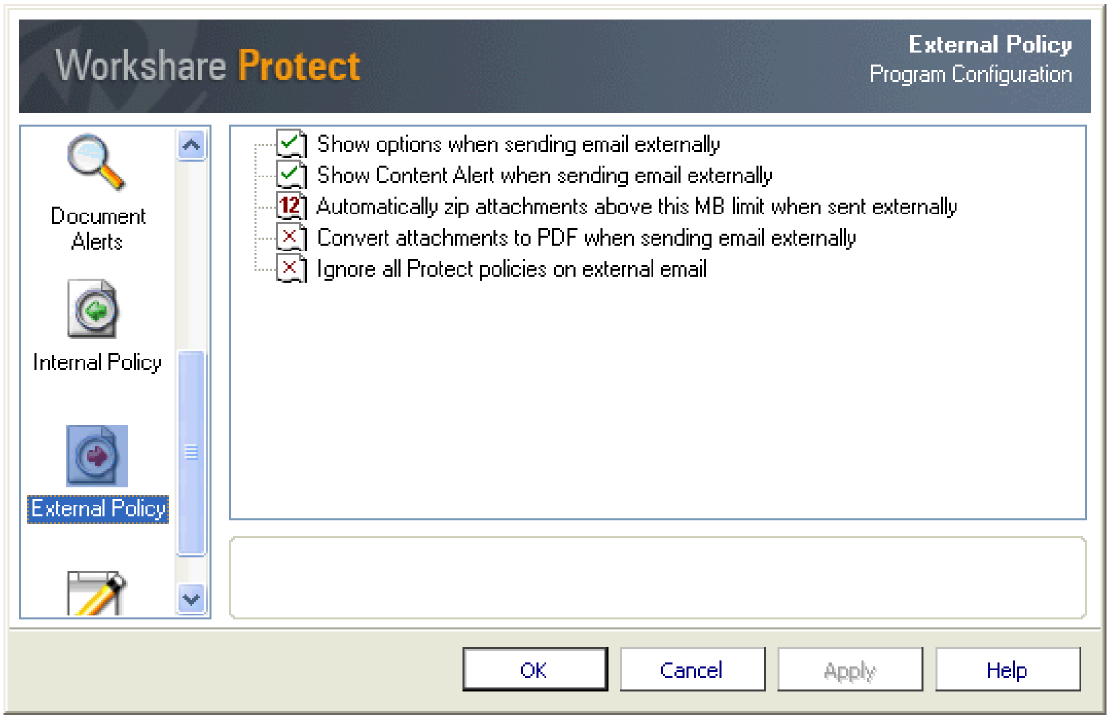
Parameter	Description
Show Content Alert when sending email internally	If selected, users will be alerted when they attempt to send documents internally that contain high, medium or low levels of hidden data. This parameter is not selected by default.
Automatically zip attachments above this MB limit when sent internally	If selected, documents attached to the email are automatically zipped when above the specified MB limit and the email is sent internally. The default setting is blank, so automatic zipping does not occur. ***Note:*** *As long as at least one of the attachments is in one of the following formats then ALL the attachments are zipped: DOC, RTF, XLS or DOT.*
Convert attachments to PDF when sending email internally	If selected, Microsoft Office documents attached to the email are automatically converted to PDFs when the email is sent internally. When **Show options when sending email internally** is selected, the user can select at the time of the send if the documents should be converted or not, and overwrite the default setting selected here.
Ignore all Protect policies on internal email	If selected, Workshare Protect will NOT check the content and attachments of emails sent internally to see if they breach any security policies. By default, this parameter is selected.
Treat the following addresses as internal	You can specify any email addresses here that you would like to be treated as internal for the purpose of Workshare Protect applying policies. Separate multiple addresses with a semi-colon.

External Policy

This category is available in the Workshare Policy Configuration Manager.

The **External Policy** category includes parameters that enable you to specify the policy to be applied when sending emails to external recipients.

> ***Note:*** *When specifying parameters in the* ***External Policy*** *category, bear in mind that where emails are sent to multiple recipients and at least one is an external recipient, then external policy settings are applied.*



☑ Show options when sending email externally
☑ Show Content Alert when sending email externally
12 Automatically zip attachments above this MB limit when sent externally
☒ Convert attachments to PDF when sending email externally
☒ Ignore all Protect policies on external email

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The External Policy parameters are described in the following table:

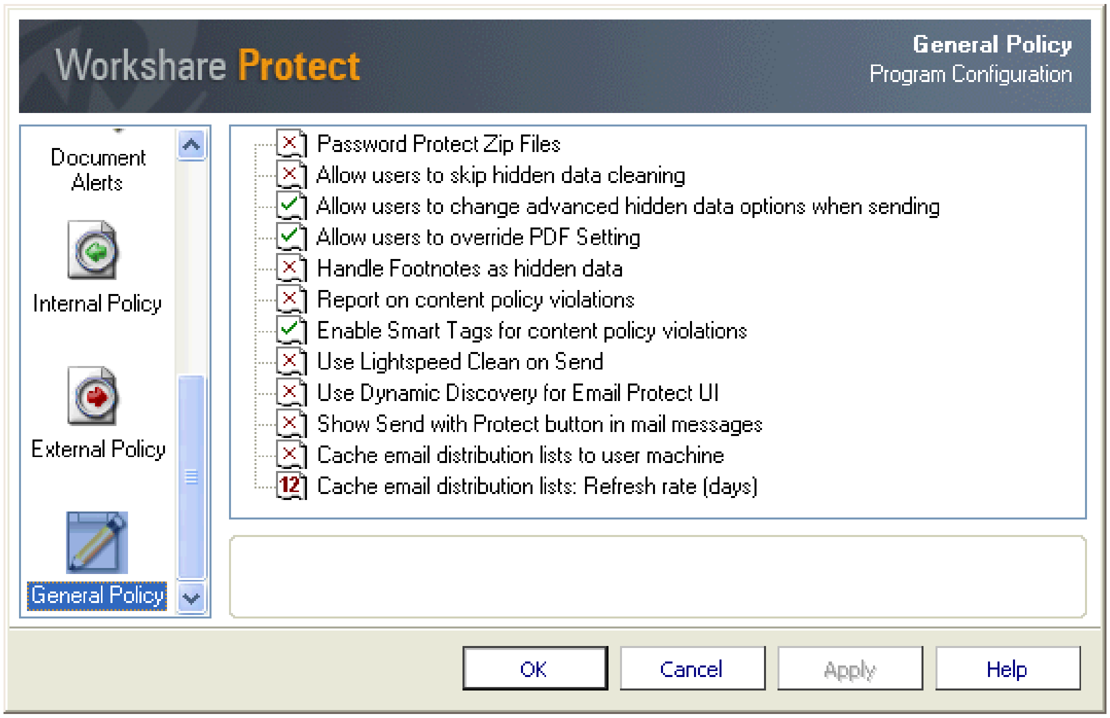
Parameter	Description
Show options when sending email externally	If selected, users will see the *Email Security* dialog with options to convert to PDF or remove hidden data when they send documents to external users. When this setting is not selected, users will not see the *Email Security* dialog and the email is processed according to the hidden data cleaning and PDF options specified in the configuration. By default, this parameter is selected so the *Email Security* dialog is displayed when emailing to external users.
Show Content Alert when sending email externally	If selected, users will be alerted when they attempt to send documents externally that contain high, medium or low levels of hidden data. This parameter is selected by default.

Parameter	Description
Automatically zip attachments above this MB limit when sent externally	The size limit for zipping attachments sent to external recipients. If this option is left blank, no zipping is done. If this option is set to 0, attachments are always zipped (unless they are already zipped). You can also set this value to a particular size, for example, 0.5. In this case zipping only occurs if attachments are larger than 0.5MB. The default setting is blank, so automatic zipping does not occur. ***Note:*** *As long as at least one of the attachments is in one of the following formats then ALL the attachments are zipped: DOC, RTF, XLS or DOT.*
Convert attachments to PDF when sending email externally	If selected, Microsoft Office documents attached to the email are automatically converted to PDFs when the email is sent externally. When **Show options when sending email externally** is selected, the user can select at the time of the send if the documents should be converted or not, and overwrite the default setting selected here.
Ignore all Protect policies on external email	If selected, Workshare Protect will NOT check the content and attachments of emails sent externally to see if they breach any security policies. By default, this parameter is NOT selected.

General Policy

This category is available in the Workshare Policy Configuration Manager.

The **General Policy** category includes parameters that enable you to specify the policy to be applied when sending emails.



- ☒ Password Protect Zip Files
- ☒ Allow users to skip hidden data cleaning
- ☑ Allow users to change advanced hidden data options when sending
- ☑ Allow users to override PDF Setting
- ☒ Handle Footnotes as hidden data
- ☒ Report on content policy violations
- ☑ Enable Smart Tags for content policy violations
- ☒ Use Lightspeed Clean on Send
- ☒ Use Dynamic Discovery for Email Protect UI
- ☒ Show Send with Protect button in mail messages
- ☒ Cache email distribution lists to user machine
- 12 Cache email distribution lists: Refresh rate (days)

The parameters are displayed in the upper area of the right pane. Selecting a parameter enables you to specify that parameter in the lower area of the right pane.

The General Policy parameters are described in the following table:

Parameter	Description
Password Protect Zip Files	If selected, users are prompted to enter a password whenever attachments are automatically zipped. This option is used in conjunction with the automatic zip options. When this setting is not selected, zip files are not password-protected.
Allow users to skip hidden data cleaning	If selected, the **Skip Cleaning** checkbox is enabled in the *Email Security* dialog. This option enables the user to omit all hidden data cleaning.
Allow users to change advanced hidden data options when sending	If selected, the **Remove Comments** and the **Remove Track Changes** checkboxes as well as the **Hidden Data Options** tab are available in the *Email Security* dialog. These options enable the user to specify exactly which hidden data types to remove from an attachment.
Allow users to override PDF Setting	If selected, the **Convert to PDF** checkbox as well as the **PDF Options** tab are available in the *Email Security* dialog. These options enable the user to specify whether or not to convert an attachment to PDF and what, if any, PDF security settings to apply.
Handle Footnotes as hidden data	If selected, footnotes are also treated as hidden data. You will be able to see the number of footnotes in a document in the Send Draft For Review page and also see details of the footnotes in a document in the Content Risk page.
Report on content policy violations	Microsoft Word only. If selected, Workshare Protect will search your documents for sensitive information that may violate your company's information security policy. Workshare Protect will report on the discovery of information such as credit card numbers, social security numbers, revenue information and profanity. Workshare Protect reports but does not remove this content.
Enable Smart Tags for content policy violations	Microsoft Office 2003 only. If selected, Workshare Protect enhances the Microsoft Word smart tags functionality to enable you to review content policy violations in a document. Microsoft Word recognizes certain types of data and labels it with a smart tag (a purple dotted underline). Workshare Protect expands the types of data recognized so that potential content policy violations in a document are indicated by the use of a smart tag.
Use Lightspeed Clean on Send	If selected, when an email or its attachment triggers a Clean action, Workshare will perform a Lightspeed clean. This type of cleaning is faster than a regular clean. This parameter is NOT selected by default.
Use Dynamic Discovery for Email Protect UI	If selected, when a user sends an email, the *Email Security* dialog is displayed immediately while Workshare Protect scans the email, and the actions are enabled once the scanning is complete. When this setting is not selected, a progress bar is first displayed and the *Email Security* dialog is only displayed once the scanning is complete. This parameter is NOT selected by default.

Parameter	Description
Show Send with Protect button in mail messages	If selected, a **Send and Protect** button is displayed in email messages. Clicking this button enables the user to always access the *Email Security* dialog (regardless of policy settings) and specify cleaning or converting to PDF of attachments as required. ***Note**: This button is not available in Microsoft Outlook 2003 when Microsoft Word is set as the email editor.* This parameter is NOT selected by default.
Cache email distribution lists to user machine	If selected, once Workshare Protect has resolved a distribution list (determined if it should be treated as external or internal), the results are stored locally. In this way, when the distribution list is used again, Workshare Protect can quickly determine whether to treat the email as internal or external. In addition, if this parameter is selected, when Microsoft Outlook is launched Workshare Protect will resolve all distribution lists in the global address book and store the results. This is done in the background. This parameter is NOT selected by default.
Cache email distribution lists: Refresh rate (days)	This parameter is relevant when the **Cache email distribution lists to user machine** parameter is selected. The results from resolving distribution lists are refreshed after the specified number of days. The default setting is 30 days.

Registry Configuration

This section describes configuration of Workshare Protect that is done by making changes in the Registry.

***Important:** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Only system administrators should attempt to make changes in the Registry.*

Clean Before PDF

When creating PDF files with Workshare Protect, the user can select to clean metadata from the document by selecting the **Clean before PDF** checkbox in the *PDF Security Options* dialog. If you want Workshare Protect to remember the user's selection when the *PDF Security Options* dialog is opened again, you need to create the **CleanBeforePDF** Registry key in the following location: HKEY_CURRENT_USER\\SOFTWARE\\Workshare\\Professional\\Settings. The value (DWORD) can be set to either 1 or 0.

Convert Hyperlinks

When converting documents to PDF files, the Workshare PDF driver does not by default convert hyperlinks. Some PDF reader will convert hyperlinks within a PDF. However, if you want the Workshare PDF driver to convert hyperlinks when creating the PDF, you need to create the **ConvertHyperlinks** Registry key in the following location: HKEY_LOCAL_MACHINE\SOFTWARE\Workshare\Professional\Settings. The value (DWORD) must be set to 1. Note that enabling this feature will impact performance and will slow down the PDF conversion process.

Sample Typical Configuration Options

This section describes how to configure some typical configuration scenarios.

Clean and PDF Silently (No Progress Bar)

This scenario configures Workshare Protect as follows:

- The **Send and Protect** button is available in email message windows – when clicked, the Workshare Protect *Email Security* dialog is displayed.
- When the Microsoft Outlook **Send** button is clicked, Workshare Protect cleans and converts to PDF all attachments using the default settings when the email is sent externally. No progress bar is displayed to the user.

To set up this scenario, configure Workshare Protect as follows:

In the Workshare Application Configuration Manager:

Category	Parameter	Setting
Administration	Show Progress Dialog on Send	NOT selected

In the Workshare Policy Configuration Manager:

Category	Parameter	Setting
Internal Hidden Data Removal		All High/Medium/Low Risk Elements NOT selected
External Hidden Data Removal		All High/Medium/Low Risk Elements selected as required
Internal Policy	Ignore restriction settings on internal email	Selected
	Show options when sending email internally	NOT selected
	Show Content Alert when sending email internally	NOT selected
	Convert attachments to PDF when sending email internally	NOT selected
	Ignore all Protect policies on internal email	Selected

Category	Parameter	Setting
External Policy	Show options when sending email externally	NOT selected
	Show Content Alert when sending email externally	NOT selected
	Convert attachments to PDF when sending email externally	Selected
	Ignore all Protect policies on external email	NOT selected
General Policy	Show Send with Protect button in mail messages	Selected

Clean and PDF Silently (With Progress Bar)

This scenario configures Workshare Protect as follows:

- The **Send and Protect** button is available in email message windows – when clicked, the Workshare Protect *Email Security* dialog is displayed.
- When the Microsoft Outlook **Send** button is clicked, Workshare Protect cleans and converts to PDF all attachments using the default settings when the email is sent externally. A progress bar is displayed to the user.

To set up this scenario, configure Workshare Protect as follows:

In the Workshare Application Configuration Manager:

Category	Parameter	Setting
Administration	Show Progress Dialog on Send	Selected

In the Workshare Policy Configuration Manager:

Category	Parameter	Setting
Internal Hidden Data Removal		All High/Medium/Low Risk Elements NOT selected
External Hidden Data Removal		All High/Medium/Low Risk Elements selected as required
Internal Policy	Ignore restriction settings on internal email	Selected
	Show options when sending email internally	NOT selected
	Show Content Alert when sending email internally	NOT selected
	Convert attachments to PDF when sending email internally	NOT selected
	Ignore all Protect policies on internal email	Selected
External Policy	Show options when sending email externally	NOT selected
	Show Content Alert when sending email externally	NOT selected

Category	Parameter	Setting
	Convert attachments to PDF when sending email externally	Selected
	Ignore all Protect policies on external email	NOT selected
General Policy	Show Send with Protect button in mail messages	Selected

Enforced Cleaning and PDF Conversion (User is Informed of Actions)

This scenario configures Workshare Protect as follows:

- The **Send and Protect** button is available in email message windows – when clicked, the Workshare Protect *Email Security* dialog is displayed.
- When the Microsoft Outlook **Send** button is clicked and the email is sent externally, the Workshare Protect *Email Security* dialog is displayed. The user can see that Workshare Protect will clean and convert to PDF all attachments using the default settings but the user cannot override these settings. A progress bar is displayed to the user.

To set up this scenario, configure Workshare Protect as follows:

In the Workshare Application Configuration Manager:

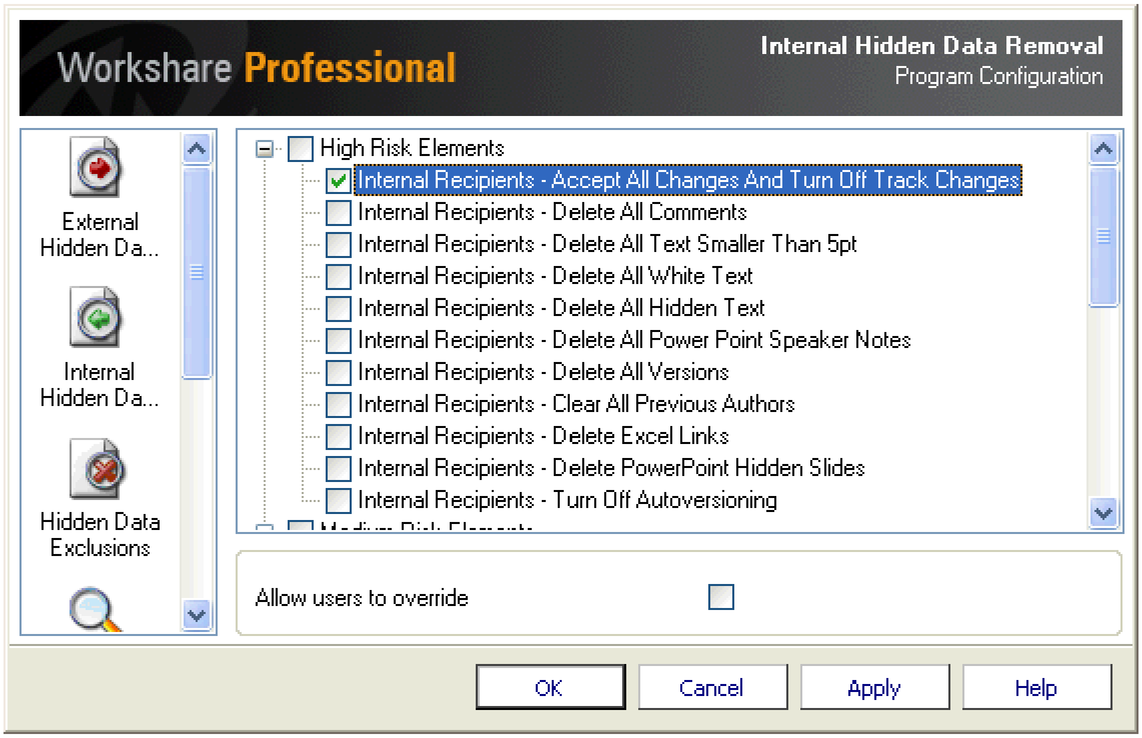
Category	Parameter	Setting
Administration	Show Progress Dialog on Send	Selected

In the Workshare Policy Configuration Manager:

Category	Parameter	Setting
Internal Hidden Data Removal		All High/Medium/Low Risk Elements NOT selected
External Hidden Data Removal	See Note below table	All High/Medium/Low Risk Elements selected as required
Internal Policy	Ignore restriction settings on internal email	Selected
	Show options when sending email internally	NOT selected
	Show Content Alert when sending email internally	NOT selected
	Convert attachments to PDF when sending email internally	NOT selected
	Ignore all Protect policies on internal email	Selected
External Policy	Show options when sending email externally	Selected
	Show Content Alert when sending email externally	NOT selected

Category	Parameter	Setting
	Convert attachments to PDF when sending email externally	Selected
	Ignore all Protect policies on external email	NOT selected
General Policy	Show Send with Protect button in mail messages	Selected
	Allow users to override PDF Setting	NOT selected

> ***Note**: For every parameter selected, ensure that the **Allow users to override** option is NOT selected. An example is shown below.*



- □ High Risk Elements
  - ☑ Internal Recipients - Accept All Changes And Turn Off Track Changes
  - □ Internal Recipients - Delete All Comments
  - □ Internal Recipients - Delete All Text Smaller Than 5pt
  - □ Internal Recipients - Delete All White Text
  - □ Internal Recipients - Delete All Hidden Text
  - □ Internal Recipients - Delete All Power Point Speaker Notes
  - □ Internal Recipients - Delete All Versions
  - □ Internal Recipients - Clear All Previous Authors
  - □ Internal Recipients - Delete Excel Links
  - □ Internal Recipients - Delete PowerPoint Hidden Slides
  - □ Internal Recipients - Turn Off Autoversioning

Allow users to override □

Cleaning and PDF Conversion on Demand

This scenario configures Workshare Protect as follows:

- The **Send and Protect** button is available in email message windows – when clicked, the Workshare Protect *Email Security* dialog is displayed.
- When the Microsoft Outlook **Send** button is clicked, emails to internal and external users are sent with no Workshare Protect interaction. In other words, Workshare Protect does not clean or convert to PDF any attachments and no progress bar is displayed to the user.

To set up this scenario, configure Workshare Protect as follows:

In the Workshare Application Configuration Manager:

Category	Parameter	Setting
Administration	Show Progress Dialog on Send	NOT selected

In the Workshare Policy Configuration Manager:

Category	Parameter	Setting
Internal Hidden Data Removal		All High/Medium/Low Risk Elements NOT selected
External Hidden Data Removal		All High/Medium/Low Risk Elements NOT selected
Internal Policy	Ignore restriction settings on internal email	Selected
	Show options when sending email internally	NOT selected
	Show Content Alert when sending email internally	NOT selected
	Convert attachments to PDF when sending email internally	NOT selected
	Ignore all Protect policies on internal email	Selected
External Policy	Show options when sending email externally	NOT selected
	Show Content Alert when sending email externally	NOT selected
	Convert attachments to PDF when sending email externally	NOT selected
	Ignore all Protect policies on external email	Selected
General Policy	Show Send with Protect button in mail messages	Selected

Note*: If you want to configure Workshare Protect to provide different actions when a user clicks the* ***Send and Protect*** *button, please contact Workshare Technical Support.*

Chapter 4. Integration

This chapter describes how to integrate Workshare Protect with your email systems. It includes the following sections:

- **Introduction**, below, introduces integrating Workshare Protect with your email systems.
- **Email System Integration**, page 67, describes how to integrate Workshare Protect with your email system.

Introduction

Workshare Protect works with the following email systems:

- Microsoft XP/2003/2007
- IBM Lotus Notes 6 to 7.02, with Domino Server 6.5.3 and 7.0

During installation, Workshare Protect automatically detects your email system and configures itself to work with that system. If you work with both Lotus Notes and Microsoft Outlook, Workshare Protect is configured to work with Lotus Notes.

Workshare Protect and SafetyGain Compatibility

Users who have SafetyGain installed and intend to install Workshare Protect should read and apply the following points:

- It is recommended that users who already have SafetyGain installed, should set their slowdocs setting to 1 in their sfnet.ini file when Workshare Protect is deployed. For example slowdocs=1.
- Users who already have SafetyGain installed must set the **Initiate StartDocs with most of API calls** to ON when Workshare Protect is deployed. This can be found by selecting **Options** and then **Preferences** on the SafteyGain desktop and then selecting the **Advanced Options** tab. If this is not set then users may get SQL connectivity errors after installing Workshare Protect.

Email Systems Integration

Workshare uses the mail server address book to determine if recipients are internal or external, and applies particular settings as a result. Therefore if you want to use Workshare Protect to protect your documents while working offline, you need to ensure your machine is set up to enable recipients to be resolved correctly.

If a copy of your mail server address book is not available locally, all recipients are treated as external. The following sections describe how to create a local copy of your mail server address book in different email clients.

Setting Up Microsoft Outlook

For Workshare Protect to work correctly with Microsoft Outlook in offline mode, you simply need to enable offline mode (as specified in the Microsoft Outlook documentation), and ensure that you download the server address book.

To download the server address book:

1. From the *Tools* menu, select **Send/Receive** and then **Download Address Book**.
2. Select to download the address book.
3. Select to download full details.
4. Ensure the correct server address book is selected.

Setting Up Lotus Notes

For Workshare Protect to work correctly with Lotus Notes in offline mode, you need to set up the client to work offline (as specified in the Lotus Notes documentation), and set up the Mobile Directory Catalog on the Lotus Domino server. You must then replicate the Mobile Directory Catalog on the Lotus Notes client.

Setting Up the Mobile Directory Catalog on the Lotus Domino Server

This step involves creating the database (Mobile Directory Catalog), configuring the database and then loading the database.

To create the Mobile Directory Catalog:

1. From the *File* menu, select **Database** and then **New**.
2. Next to **Server**, select the Dircat server you picked to aggregate the directory catalog.
3. Next to **Title**, enter a title for the directory catalog (**Mobile Directory Catalog**).
4. Next to **Filename**, enter a file name for the catalog (‘**MobileDC.nsf**’).
5. Select **Create full text index for searching**.
6. Change **‘Template Server…’** to **Domino server**.
7. Select **Show advanced templates**.
8. Below **Template server**, select a server that stores the Directory Catalog template, and then click **OK**.
9. Select the **Directory Catalog (DIRCAT5.NTF)** template.
10. Click **OK**.

To configure the Mobile Directory Catalog:

1. In the database you created (**Mobile Directory Catalog**), select **Create** and then **Configuration**.
2. Complete the following fields in the Directory Catalog Configuration document:
   - Change **Directories to include** to include the Domino Directories the Dircat task aggregates (Names.nsf).
   - Change **Additional fields to include** to include MailSystem.
3. Click **Save** and **Close**.

To load the Mobile Directory Catalog:

- From the Lotus Domino Server Administrator run the command **Load Dircat database** to build the condensed Directory Catalog (**Load DirCat MobileDC.nsf**).

Replicating the Mobile Directory Catalog on the Lotus Notes Client

This step involves replicating the Mobile Directory Catalog on the Lotus Notes client and setting up the client to use the Mobile Directory Catalog for name resolution.

To replicate the Mobile Directory Catalog:

1. From the *File* menu, select **Database** and then **Open**.
2. In the *Open Database* dialog, change the **Server** to the Domino server and the **Database** to Mobile Directory Catalog and click **Open**.
3. While the Mobile Directory Catalog database is open, from the *File* menu, select **Replication** and then **New Replica**.
4. Verify that the server is **Local** and the file name and title is for the Mobile Directory Catalog (**MobileDC.nsf**) and click **OK**.

To set up the client to use the Mobile Directory Catalog for name resolution:

1. From the *File* menu, select **Preferences** and then **User Preferences**.
2. Select **Mail and News**.
3. Modify the **Local Address Books** and add the Mobile Directory Catalog to the existing list (**names.nsf, MobileDC.nsf**).
4. Click **OK**.

> ***Note:*** *This step can only be completed if the Mobile Directory Catalog exists. See* Setting Up the Mobile Directory Catalog on the Lotus Domino Server, *page 68.*

Issues with Custom Forms (Recipient Fields)

If you work with custom forms and you modify recipients, you should be aware of which address fields Workshare Protect uses to resolve recipients as internal or external.

In order to determine the internal/external classification of a destination, only the following fields relating to recipients are extracted from the form by the EM_MAILSENDNOTE event:

- **EnterSendTo**
- **EnterCopyTo**
- **EnterBlindCopyTo**

If you use custom forms, you should note that the fields **Recipients**, **SendTo**, **CopyTo** and **BlindCopyTo** are not resolved.

Chapter 5. Network Deployment

This chapter describes how to install and license Workshare Protect across your network. It includes the following sections:

- **Overview**, below, introduces the options available for installing Workshare Protect across a network.
- **Deploying via the Command Line**, page 73, describes the steps required to use the command line to install and license Workshare Protect across your network.
- **Citrix Installation Guidelines**, page 78, describes how to install Workshare Protect on Citrix.
- **Active Directory Deployment Guidelines**, page 79, describes how to deploy Workshare Protect using Active Directory.
- **SMS Deployment Guidelines**, page 87, describes how to deploy Workshare Protect using SMS.

Overview

Deploying Workshare Protect across your network means installing and licensing Workshare Protect on all workstations in your network. Workshare Protect can be deployed across your network using the Workshare Protect command line installation or third party deployment products.

It is recommended to deploy Workshare Protect in a licensed state and to that end the following procedures describe how to set the LICFILE property. However, you could also license Workshare Protect after installation. Refer to *Licensing Workshare Protect*, page 25. Additionally, if you want to deploy specific configuration settings with Workshare Protect, you must set the INIFILE property. Refer to *Chapter 3: Configuration.*

The main install now downloads prerequisites from the Internet if they are required. For enterprise deployments, the prerequisites have been bundled into a zip file (**WorksharePrereqsFor522.zip**). To skip downloading files from the Internet, the prerequisites can be extracted to the same location as the extracted files from the main installation files.

Installation File Summary

The installation requires the following prerequisites:

Prerequisite	Version	OS	Office	Notes
Windows Installer	3.1.0.0	Windows XP, Server 2003	NA	
Microsoft .NET Framework 3.0	3.0.4506.30	Windows XP, Server 2003	NA	Microsoft .NET Framework 3 contains Microsoft .NET Framework 2 and MSXML 6.0.
KB908002 - Shared Add-in Support Update for Microsoft .NET Framework 2.0	1.0.0	NA	All versions	This KB is required for Microsoft Office to load .NET add-ins.

Prerequisite	Version	OS	Office	Notes
MSXML 6.0	NA	NA	NA	This prerequisite is installed by the Microsoft .NET Framework 3 install.
Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x86)	8.0.5193	All (including x64 versions)	NA	
Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x64)	8.0.5192	x64 OS versions	NA	The right-click handler is written in x64 code and requires this prerequisite.
Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x86)	9.0.30729.4148	All (including x64 versions)	NA	
Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x64)	9.0.30729.4148	x64 OS versions	NA	The right-click handler is written in x64 code and requires this prerequisite.
Microsoft Report Viewer (x86)	8.0.50727.42	All	NA	
KB907417 – Update for Office 2003	1.0.0	NA	Office 2003	
KB935514 – Update for Office 2007	1.0.0	NA	Office 2007 pre SP1 only	
Microsoft Office System Primary Interop Assemblies (PIA)	12.0.4518.1014	NA	Office 2007	
Open XML Format SDK	1.0.1825	All	NA	
Windows Installer for Server 2003 (x64)	3.1	Windows Server 2003 x64	n/a	http://www.microsoft.com/downloads/details.aspx?FamilyId=8B4E6B93-1886-4D47-A18D-35581C42ECA0&displaylang=en
Windows Installer for Server 2003 (x86)	3.1	Windows Server 2003 x86	n/a	http://www.microsoft.com/downloads/details.aspx?FamilyId=8B4E6B93-1886-4D47-A18D-35581C42ECA0&displaylang=en

> ***Note:*** *Windows Installer and Microsoft .NET Framework should be installed first. The other prerequisite components can be installed in any order.*

The extracted files include the following Workshare MSI packages:

- Workshare PDF Converter, version 5.0.159 [WorksharePdfConverter.msi]
- Workshare Protect Client, version 5.22 [WorkshareProtect.msi]

The extracted files include the following Workshare files which can be used to install Workshare Protect:

- Workshare.InstallWizard.exe
- Workshare.InstallWizard.ini

The Workshare.InstallWizard.exe uses the Workshare.InstallWizard.ini file which contains the information required to install Workshare Protect correctly. In the INI file each package has a section which provides information about the executable such as display name, version number, installer path and installer command line arguments.

Deploying via the Command Line

You can use the executable file or the MSI files found within the executable file to install Workshare Protect from the command line.

Installation Procedure with the Install Wizard

The Workshare Protect install contains the Workshare Install Wizard and Workshare installs. Some of the prerequisites are contained in the install. The Workshare Install Wizard examines the client desktop, downloads any prerequisites not present, installs the prerequisites and installs and configures the Workshare installs.

Deploying Workshare Protect with the Self-Extracting Executable

The following procedure describes how to install Workshare Protect using the self-extracting executable.

To install Workshare Protect using the self-extracting executable:

1. Create a shared directory with relevant permissions so that client machines can access the Workshare Protect executable during the installation.
2. Copy the self-extracting executable to the shared directory.
3. Run the executable on the client desktop. This will extract the files to the client and run the Install Wizard on the client machine. Parameters passed to the self-extracting executable are passed on to the Install Wizard. The command line is:

```
<path to WorkshareProtect-9800.XXX.exe> -product “Workshare Protect” [-
autorun] [-silent] [-acceptDownload]
```

You must add ‘-acceptDownload’ to the command line if you are installing silently and there are prerequisites that need to be downloaded from the Internet. To skip downloading the prerequisites from the Internet, follow the instructions in the next section.

Deploying Workshare Protect using Extracted Contents of the Executable

The following procedure describes how to install Workshare Protect using the contents of the self-extracting executable. Extracting the contents enables customization of the install and allows the administrator to skip downloading the prerequisites by providing the prerequisites directly.

To install Workshare Protect using the extracted contents of the executable:

1. Create a shared directory with relevant permissions so that client machines can access the Workshare Protect installation files during the installation.

2. Extract the contents of the Workshare Protect executable to the directory created in step 1.

3. (Optional) Extract the contents of **WorksharePrereqsFor522.zip** to the directory creates in step 1.

4. Run the Install Wizard on the client desktop with the appropriate options. You must specify '-acceptDownload' if you have specified '-silent', you have NOT followed step 3 and prerequisites are required by the client desktop. The Install Wizard command line can be:

```
<path to Workshare.InstallWizard.exe> -product “Workshare Protect” [-
autorun] [-silent] [-acceptDownload]
```

Examples

If you want an install where the user must click through the Wizard screens, an example command would be as follows:

```
<path to Workshare.InstallWizard.exe> -product “Workshare Protect”
```

If you want an install where the progress is displayed to the user but they do not have to click through the Wizard screens, an example command would be as follows:

```
<path to Workshare.InstallWizard.exe> -product “Workshare Protect” -autorun -
acceptDownload
```

If you want an install where the progress is not displayed to the user, an example command would be as follows:

```
<path to Workshare.InstallWizard.exe> -product “Workshare Protect” -silent
-acceptDownload
```

Installation Procedure using the MSI Files Directly

To install Workshare Protect using the MSI files you must extract the contents of the Workshare Protect executable and ensure that all prerequisites are installed on the client desktop.

Installation Procedure without Install Wizard

For each file that you need to install you must retrieve the following information from the appropriate section in the Workshare.InstallWizard.ini file:

- InstallerPath
- InstallerArgs

For executables you must specify the full path to the location of the executable in InstallerPath followed by the InstallerArgs. In general this will install the executable quietly.

For MSIs you must specify msiexec.exe /i [InstallerPath] [InstallerArgs].

To deploy Workshare Protect without the Install Wizard using the command line:

1. Create a shared directory with relevant permissions so that client machines can access the Workshare Protect installation files during the installation.
2. Extract the contents of the Workshare Protect executable to the shared directory created in step 1.
3. Install prerequisites, as listed on page 71.
4. Install WorksharePdfConverter.msi.
5. Install WorkshareProtect.msi.

   In order to deploy Workshare Protect in a licensed state, the property LICFILE is set in the install string of the Protect Client. In order to deploy Workshare Protect with specific configuration settings, the property INIFILE is set. Refer to *Chapter 3: Configuration* for information on creating and saving configuration (INI) files.

> ***Note:*** *The Workshare Protect MSIs must be installed in the order specified above.*

Example Installation

The following example will install Workshare Protect for the first time on a system that requires .NET 3 Framework quietly. This is done from the command line, from within a DOS window or using a batch (.bat) file and should only be attempted by the network administrator or other qualified personnel. It assumes that the files have been extracted to a shared directory.

To install Workshare Protect:

1. Enter the following command to install the .NET 3 Framework quietly:

   ```
   <path to shared directory>dotnetfx3.exe /q:u /c:”install /q /l”
   ```

2. Enter the following command to install the Pdf Converter quietly:

   ```
   msiexec.exe /i <path to shared directory>\WorksharePdfConverter.msi /qn
   ```

3. Enter the following command to install the Protect Client quietly:

   ```
   msiexec.exe /i <path to shared directory>\WorkshareProtect.msi
   REINSTALL=ALL REINSTALLMODE=vomus ALLUSERS=1 SKIP_UPGRADE_WARNING=1
   <property1> <property2> <property…> /qn
   ```

> ***Note:*** *If you want to turn logging on during the install, add* ***/l*v <path and name of log file>*** *before /***qn***. This generates a Windows Installer verbose (descriptive) log file which can be useful should you need to contact Workshare Technical Support.*

As an alternative to installing quietly (/qn) the following msiexec command line arguments can be used:

/qn+ = silent install with final notification

/qb = basic interface installation

/qr = reduced interface installation

Refer to *Appendix A: Additional Msiexec.exe Parameters and Switches*, for additional parameters and switches that can be passed to the msiexec.exe.

Compulsory Properties

The following tables shows the compulsory properties that must be specified and which MSI they relate to.

Property	MSI	Value
REINSTALL	PDF Converter Protect	Ensures that upgrades install correctly. The required value is **ALL**.
REINSTALLMODE	PDF Converter Protect	Sets the reinstall mode for upgrades. The default value is **vomus**. This ensures that the latest versions of the MSI packages are cached and older files are overwritten.
ALLUSERS	PDF Converter Protect	Installs the application per machine. The default value is **1**.
INSTALLSERVICE	Not required	Installs and enables the Workshare Protect Service. The required value is **1.** **This property is no longer required but is still honored.**
INSTALLDIR	Protect	Specifies the installation folder for Workshare Protect. The default value is **<ProgramFilesFolder>\Workshare\Modules**.
SKIP_UPGRADE_WARNING	Protect	Disables the display of the upgrade warnings when installing Workshare Protect. The required value is **1.**

Protect Client Properties

The following tables shows the optional properties that can be specified to the Protect Client install.

Property	Value
INIFILE	Name and location of the configuration file. For example, **INIFILE=”\\server\share\inifile.ini”**. The specified INI file is loaded and applied. For further information on the INI file, refer to *Chapter 3: Configuration*. ***Note:*** *If you manually copy an INI file into the* ***Modules\Config*** *folder of the Workshare Protect installation directory folder, it will be applied when the Workshare Configuration Assistant is run. It will not be reapplied if the Workshare Configuration Assistant is run again, as it caches the time stamp on the INI file.*
LOGFILE	Name and location of the WCA log file. For example, **LOGFILE=”C:WorkshareConfig.log”**. The log file can either be stored at a shared location or stored locally on the workstation. If a location is not specified for the log file it will be written to the local TEMP folder. By default the log file is named **WorkshareConfig.log**. The WCA log file will provide details of all the steps the WCA has taken and can be passed to Workshare if any difficulties are encountered. The log file is appended to, not overwritten, in order to retain all logged information. Therefore the latest details will be at the end of the log file.
LICFILE	Name and location of the license file. For example, **LICFILE=”\\server\share\Workshare.lic”**. The specified LIC file will be copied to the **Modules** folder of the Workshare Protect installation directory. ***Note:*** *The most recent license file will be used by Workshare Protect.*
NOTESINIFILE_PATH	Location of the notes.ini file. This should be specified in non-standard IBM Lotus Notes environments to ensure that Workshare components are added correctly to the INI file by the install.
INSTALL_EXCEL_ INTEGRATION	Integrates Workshare Protect into Microsoft Excel. To enable installation of the Microsoft Excel integration, set INSTALL_EXCEL_INTEGRATION=ON.
INSTALL_POWERPOINT_ INTEGRATION	Integrates Workshare Protect into Microsoft PowerPoint. To enable installation of the Microsoft PowerPoint integration, set INSTALL _POWERPOINT_INTEGRATION=ON.
INSTALL_WORD_ INTEGRATION	Integrates Workshare Protect into Microsoft Word. To enable installation of the Microsoft Word integration, set INSTALL_WORD_INTEGRATION=ON.

If none of the Microsoft Office integrations is specified, then all integrations are installed and Workshare Protect will integrate with Microsoft Word, PowerPoint and Excel. If one of the Microsoft Office integrations is specified, then the others are assumed to be "off" unless specifically specified as "on".

> ***Notes**: The **Save templates in STARTUP folder** option can be turned on by creating the following Registry key: **SaveTemplatesToStartupFolder** with a DWORD value of **1** in the following Registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Workshare\Framework\Settings. You must create this Registry key before running the Workshare Protect installer.*
>
> *For further information about the Microsoft Office integration options and the **Save templates in STARTUP folder** option, see page 20.*

Example Workshare Protect Client Install Command Line

An example of a Workshare Protect Client installation command line is as follows:

```
msiexec.exe /i "\\InstallMachine\Workshare\WorkshareProtect.msi" REINSTALL=ALL
REINSTALLMODE=vomus ALLUSERS=1 INIFILE="\\InstallMachine\
Workshare\Workshare.ini" LOGFILE="\\InstallMachine\Workshare\Workshare.log"
LICFILE="\\InstallMachine\Workshare\Workshare.lic"
```

> ***Note:** Properties and values are all case sensitive.*
> *The use of " " should be used where there is character spacing in file paths.*
> *When using the /qn, /qn+, /qb or /qr switches, the WCA runs but is not visible to the user.*

Citrix Installation Guidelines

Workshare Protect can be installed on a Citrix server using the standard installation process. To restrict the number of users who have access to Workshare Protect, you are required to manually modify the Registry keys.

> ***Note:** Workshare Protect is configured to install on a per machine basis and not a per user basis.*

To install Workshare Protect on the Citrix server:

1. Ensure the Terminal Server is in Install mode.
2. Install Workshare Protect on the Citrix server using the standing installation process. It is recommended that the default folder structure: "Program Files/Workshare/Modules" is retained. Refer to *Chapter 2: Installation*, page 22, for more information.
3. Remove any shortcuts from the desktop if they were created.

The above steps will install Workshare Protect for all users of the Terminal Server. To customize access to Workshare functionality, use the following approach:

Enable Specific Users: Remove Workshare integration from all Microsoft Office applications and then use a logon script deployed to specific users (using Active Directory) to reconfigure the Workshare integration when needed/necessary.

Note: *When the installation remains a per machine install, all users using the Citrix server where Workshare Protect is installed will get Workshare Protect. This may not be required and it will increase the load on the server.*

Enable Specific Users

These steps are best performed immediately after installation of Workshare Protect.

To disable Workshare Protect for all Microsoft Office 2007/2003/XP users:

1. Merge the (Read Admin Guide)Citrix_Protect_LM_Remove.reg file into the Registry.
2. Check the HKEY_USERS\.DEFAULT and remove any Workshare entries.

Note: *The (Read Admin Guide)Citrix_Protect_LM_Remove.reg key also removes the shadow Registry entries which control the operation of "userinit" in terminal services environments. Refer to the following Microsoft article for further information: http://support.microsoft.com/?kbid=297379.*

To enable Workshare Protect for individual Microsoft Office 2007/2003/XP users:

- Use Active Directory to merge the Registry file (Read Admin Guide)Citrix_Protect.reg to the required user.

To remove access to Workshare Protect once granted, use Active Directory to merge (Read Admin Guide)Citrix_Protect_CU_Remove.reg file for the specific user.

Active Directory Deployment Guidelines

When working with Windows 2003 Server, you can deploy Workshare Protect across your network using Active Directory. "Assigned to machine" installation is the preferred method of distributing Workshare Protect via Active Directory and is described in the following procedure. The "assigned to user" and "published to user" methods are discussed on page 86.

Note: *Before installing using this method, please refer to the section,* Installing the MSI with the Command Line*, page 73.*
In order to deploy the non-MSI prerequisite files via Active Directory, you can create a .zap file. (See http://support.microsoft.com/kb/231747) A .zap file can be published via a group policy.

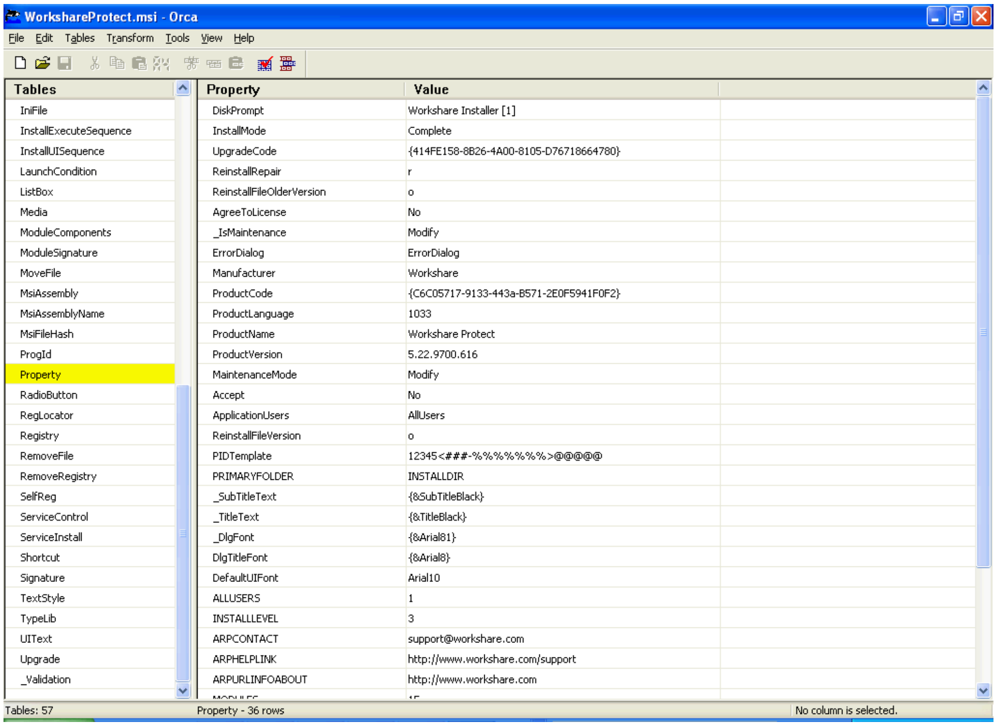
In order to deploy Workshare Protect in a licensed state, the property LICFILE is set via a Windows Installer transform file (*.mst). This step is included in the following procedure. Other properties, such as INIFILE, which specifies the configuration of Workshare Protect, can also be set via the transform file. Refer to *Chapter 3: Configuration* for information on creating and saving configuration (INI) files.

The following procedure must be completed for each of the four installation components of Workshare Protect. The following example illustrates how to create the WorkshareProtect.msi Active Directory group policy. The precedence of the group policies must be configured so that the policies are applied in the following order:

1. WorksharePDFConverter.msi
2. WorkshareProtect.msi

To deploy Workshare Protect using Active Directory:

1. On the Windows 2003 Server machine, create a shared folder with relevant permissions so that client machines can access the Workshare Protect MSI during the automatic installation.
2. Extract the MSI file (**WorkshareProtect.msi**) from the Protect install file and copy it into the folder created in step 1.
3. Create a transform (MST) file. The transform file is used to specify properties, such as LICFILE, INSTALLDIR, during the installation. The following procedure describes how to create a transform file using the Orca utility provided in the Windows Installer Software Developers Kit.
4. Launch Orca.
5. Open the WorkshareProtect.msi file.



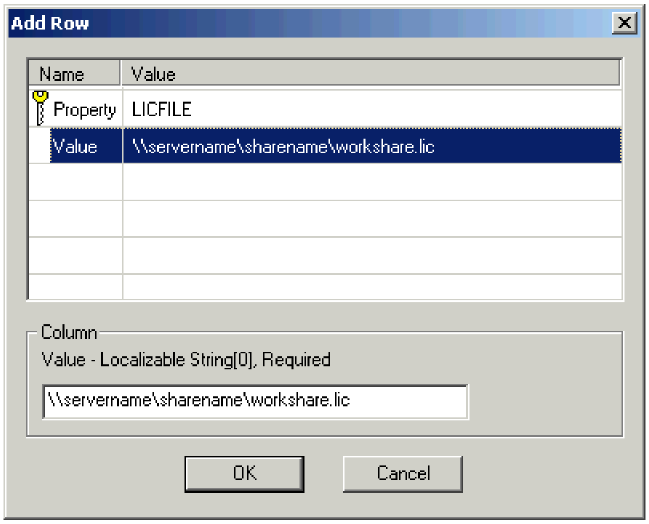
Tables	Property	Value
IniFile	DiskPrompt	Workshare Installer [1]
InstallExecuteSequence	InstallMode	Complete
InstallUISequence	UpgradeCode	{414FE158-8B26-4A00-8105-D76718664780}
LaunchCondition	ReinstallRepair	r
ListBox	ReinstallFileOlderVersion	o
Media	AgreeToLicense	No
ModuleComponents	_IsMaintenance	Modify
ModuleSignature	ErrorDialog	ErrorDialog
MoveFile	Manufacturer	Workshare
MsiAssembly	ProductCode	{C6C05717-9133-443a-B571-2E0F5941F0F2}
MsiAssemblyName	ProductLanguage	1033
MsiFileHash	ProductName	Workshare Protect
ProgId	ProductVersion	5.22.9700.616
Property	MaintenanceMode	Modify
RadioButton	Accept	No
RegLocator	ApplicationUsers	AllUsers
Registry	ReinstallFileVersion	o
RemoveFile	PIDTemplate	12345<###-%%%%%%%>@@@@@
RemoveRegistry	PRIMARYFOLDER	INSTALLDIR
SelfReg	_SubTitleText	{&SubTitleBlack}
ServiceControl	_TitleText	{&TitleBlack}
ServiceInstall	_DlgFont	{&Arial81}
Shortcut	DlgTitleFont	{&Arial8}
Signature	DefaultUIFont	Arial10
TextStyle	ALLUSERS	1
TypeLib	INSTALLLEVEL	3
UIText	ARPCONTACT	support@workshare.com
Upgrade	ARPHELPLINK	http://www.workshare.com/support
_Validation	ARPURLINFOABOUT	http://www.workshare.com

Tables: 57 Property - 36 rows No column is selected.

6. From the *Transform* menu, select **New Transform**. In the title bar of the window, **transformed by Untitled** is displayed in parenthesis after **WorkshareProtect.msi**.

7. In the left pane, select the **Property** table.

8. Right-click in the right pane and select **Add Row**.



Name	Value
Property	LICFILE
Value	\\servername\sharename\workshare.lic

Value - Localizable String[0], Required

\\servername\sharename\workshare.lic

9. Select **Property** in the upper area and enter **LICFILE** in the lower area.

10. Select **Value** in the upper area and enter the path to the license file (Workshare.lic) in the lower area. You are advised to specify this property otherwise Workshare Protect will be deployed in an unlicensed state and you will have to license it manually.

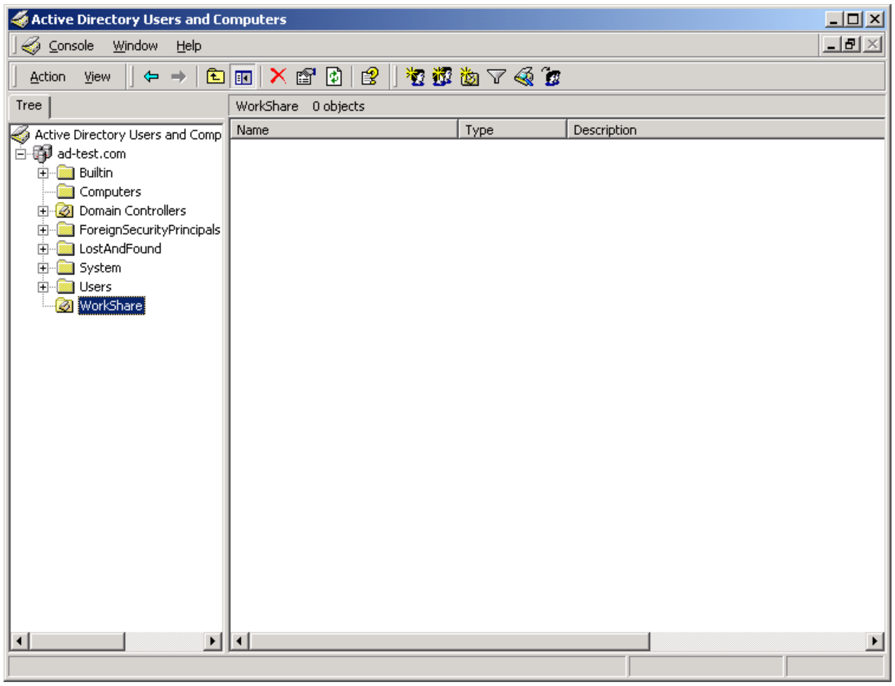
> ***Note:*** *The license file is provided by Workshare Ltd.*

11. Click **OK**.

12. Repeat steps 8 to 11 for additional properties as required. You can add any of the properties specified on page 77.

13. From the *Transform* menu, select **Generate Transform** and the save the transform file to the shared folder created in step 1.

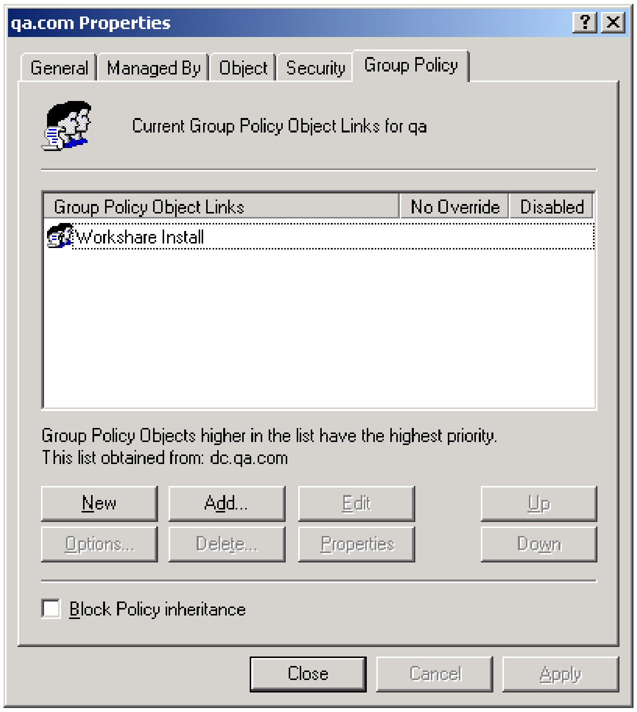
14. From the Start menu, launch **Active Directory Users and Computers**. A list of organizational units is displayed on the left side.



15. You now have to configure a group policy for the users to which you will deploy Workshare Protect. This is done for each organizational unit that includes users to which you want to deploy.

16. Right-click an organizational unit and select **Properties**.

17. In the **Group Policy** tab, click the **New** button and enter a name for the new policy (for example, **WS35Distrib**).



Current Group Policy Object Links for qa

Group Policy Object Links	No Override	Disabled
Workshare Install		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: dc.qa.com

□ Block Policy inheritance

18. Select the new policy in the upper area and click the **Properties** button.

19. In the **Security** tab, click **Add**. A list of users in the organizational unit is displayed.

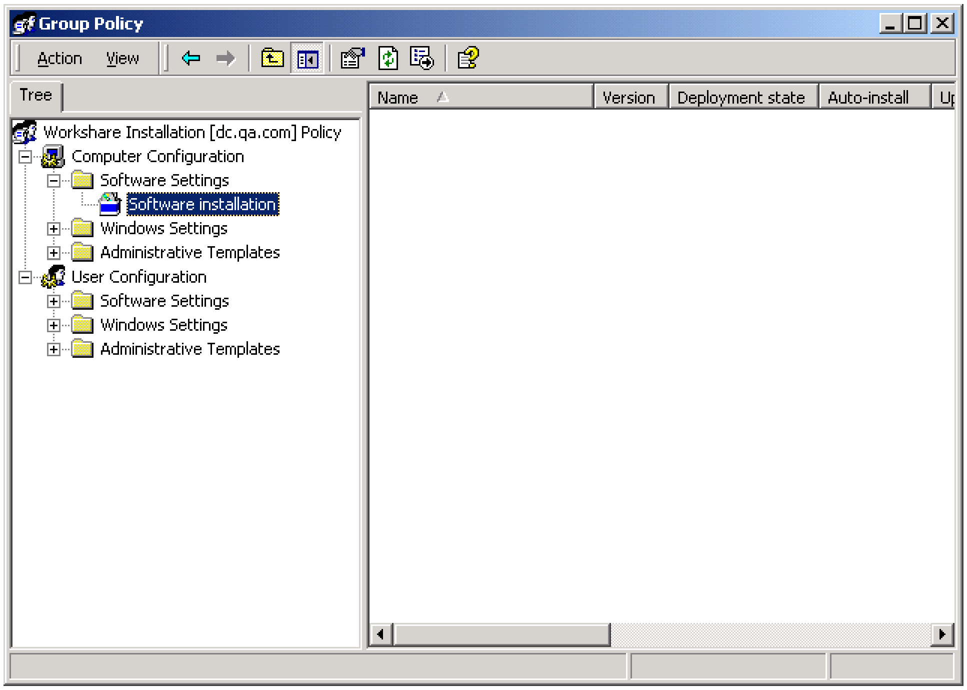
20. For all users to which you will deploy Workshare Protect, ensure that at a minimum the following permissions are selected:
    - **Read**
    - **Apply Group Policy**

21. For any users to which you do not want to deploy Workshare Protect, ensure that the **Apply Group Policy** permission is not selected.

22. Click **OK**.

23. In the **Group Policy** tab, select the policy in the upper area and click the **Edit** button. The *Group Policy* window is displayed.

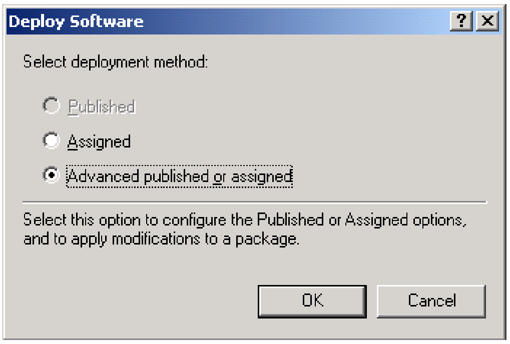
24. Expand the **Computer Configuration** tree and the **Software Settings** node.



25. Right-click **Software installation** and select **New** then **Package**.

26. Browse to the shared folder and select the WorkshareProtect.msi file.

27. Click **Open**. The *Deploy Software* dialog is displayed.



Select deployment method:

○ Published

○ Assigned

● Advanced published or assigned

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

28. Ensure that the **Advanced published or assigned** option is selected and click **OK**.

29. In the **Modifications** tab, click **Add**.

30. Browse to the transform (MST) file created in steps 4 to 13 and click **Open**.

31. Click **OK**.

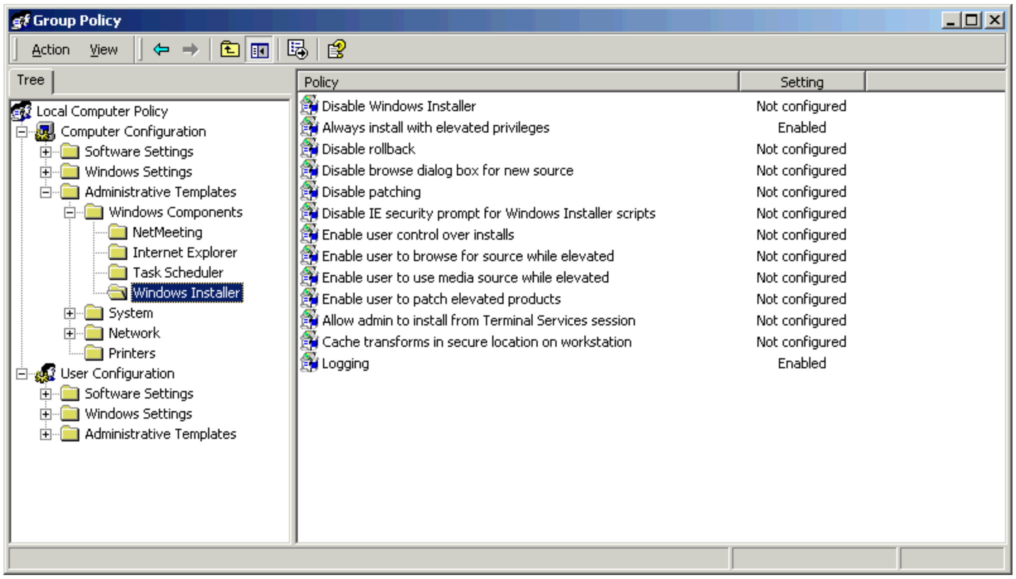
32. In the *Group Policy* window, expand the **Administrative Templates** node and then the **Windows Components** node.

33. Select **Windows Installer**.

34. On the right side of the *Group Policy* window, double-click **Logging**.

35. Select the **Enabled** radio button and in the **Logging** field, enter **voicewarmup**.

36. Click **OK**. Logging of Windows Installer is now enabled. The log file generated will be in the format **msi<random letters and numbers>.log**.

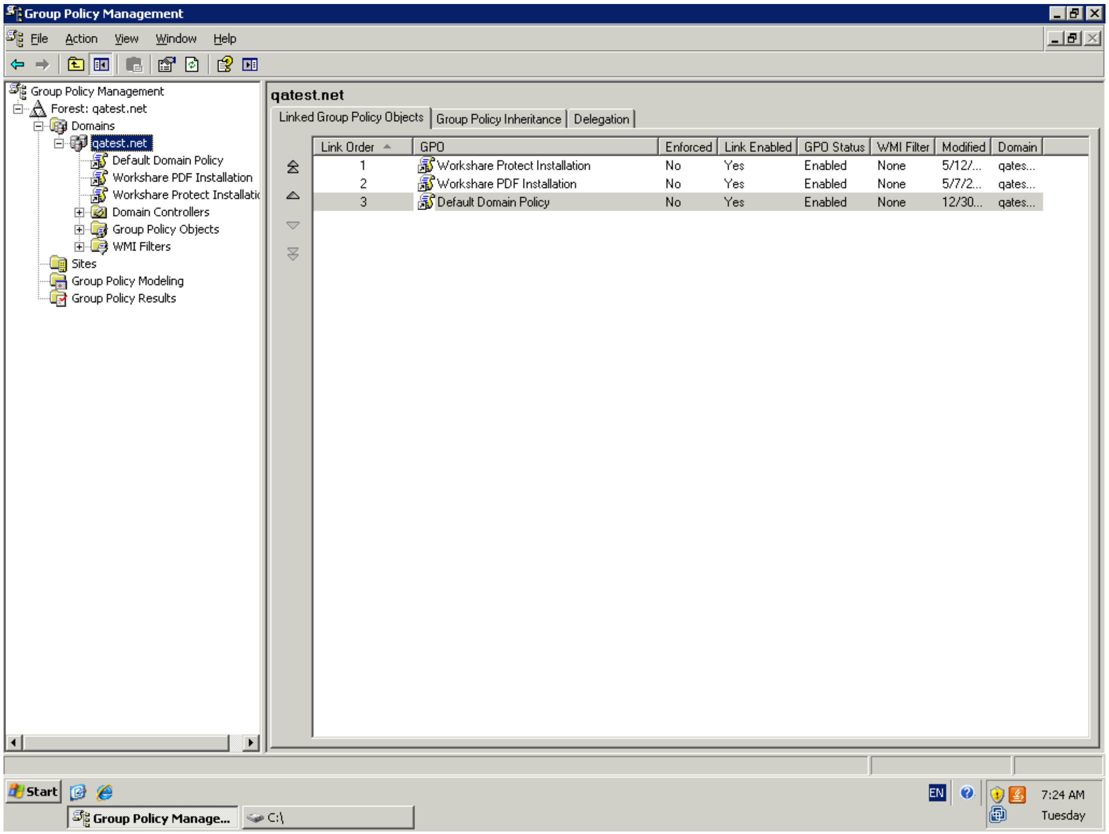


Policy	Setting
Disable Windows Installer	Not configured
Always install with elevated privileges	Enabled
Disable rollback	Not configured
Disable browse dialog box for new source	Not configured
Disable patching	Not configured
Disable IE security prompt for Windows Installer scripts	Not configured
Enable user control over installs	Not configured
Enable user to browse for source while elevated	Not configured
Enable user to use media source while elevated	Not configured
Enable user to patch elevated products	Not configured
Allow admin to install from Terminal Services session	Not configured
Cache transforms in secure location on workstation	Not configured
Logging	Enabled

37. Close the *Group Policy* window and close the organization unit's *Properties* window.

38. Repeat steps 15 to 36 for other organizational units to select all the users (machines) to which you want to deploy Workshare Protect.

Repeat the procedure above for the WorksharePDFConverter.msi. Ensure the precedence of the group policy objects is specified as shown below.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Workshare Protect Installation	No	Yes	Enabled	None	5/12/...	qates...
2	Workshare PDF Installation	No	Yes	Enabled	None	5/7/2...	qates...
3	Default Domain Policy	No	Yes	Enabled	None	12/30...	qates...

The Workshare Protect package is now ready to be deployed on a per-machine basis. The next time the client machines are rebooted, Workshare Protect will be installed.

Note: *Client machines may have to be rebooted more than once depending on their configuration.*

Assigned/Published to User Methods

In general, it is not recommended to deploy Workshare Protect using the assigned to user or published to user methods. These methods do not complement the way Workshare Protect works for the following reasons:

- If all previous installations of Workshare were assigned to machine installs, a subsequent assigned/published to user install will not remove previous versions of Workshare.
- The Workshare Protect application is not designed to support user isolation for either assigned or published to user in Active Directory deployment. Whilst Workshare Protect will operate normally for the user for which it is installed, it will also be partially visible to other users - other users on the machine will see the Workshare menu but will not be able to use it. If an application has been assigned or published to a user, another user should not be able to see it or operate it at all.

***Note:** With Workshare Protect, another user has the Workshare menu and button (not the Workshare Panel) in Microsoft Word but when a menu option or the button is clicked, the error: "**WinWord.exe Unable to perform request: Unexpected exception**" is displayed.*

Published to User

The published to user method does not install the software but it installs 'entry points' so that it looks to the user like the software is installed. However, the software is not installed until it is used - when an 'entry point' is activated, the software is installed. An 'entry point' can be things like a desktop shortcut, a start menu shortcut, a file extension or a template.

For example, if publishing Adobe Acrobat to a user, the following would happen:

- Shortcuts are placed wherever Adobe Acrobat has assigned its shortcuts (such as the desktop and start menu).
- File extension associations for PDF are linked to Adobe Acrobat.
- The software will then install if the user either attempts to click on one of the shortcuts or attempts to open a .PDF.

The published to user method uses a technology called JIT (just-in-time). This enables an administrator to deploy the software to every user (for example) and the software will only be actually installed to the users that require it. This saves on bandwidth, licensing and workstation disk space.

With Workshare Protect, there are no valid entry points.

- There are no shortcuts that users click on to launch Workshare Protect (it is opened via Microsoft Word).
- The Workshare Protect startup template is placed into the Microsoft Word Startup directory. If this were to be made into an entry point, Workshare Protect would install whenever Microsoft Word is opened which would defeat the purpose of JIT installations.
- Workshare Protect does not have a file extension other than W3 files but users will not be opening these files.

The only feature that will work with published to user is the “add new software” entry under add/remove programs.

SMS Deployment Guidelines

This section describes how to deploy Workshare Protect using Microsoft SMS 2003.

Microsoft SMS 2003 allows many different options for the deployment of applications. The following table indicates some of the principal configuration options and describes the effect of changing a given value on the installation of Workshare Protect.

Location of Option	SMS Option	Setting	Comment
Packages>Programs> Requirements Tab	"Estimated disk space"	<variable>	Optional setting – the installation will fail if the disk usage is greater than this value.
	"Maximum allowed run time"	<variable>	Optional setting – the installation will fail if it takes longer than the specified time.
	"This program can run on any platform"	On/Off	Optional setting – extra validation to ensure the program is only deployed to expected client machines.
Packages>Programs > Environment Tab	"Program can run"	"Only when a user is logged on" "Whether or not a user is logged on" "Only when no user is logged on"	Determines when the installation may be run.
	"Allow Users to interact with this program"	On/Off	Runs the installation with or without UI. This setting overwrites any other settings, eg –autorun specified when installing using the Workshare.InstallWizard.exe.
	"Run with user's rights"	On/Off	Determines credentials used to deploy application (best practice is to select "Run with administrative rights" – the installation may fail without administrative privileges).
	"Run with administrative rights"	On/Off	Best practice setting – uses specified administrative privileges to install the program.
Packages>Program> Advanced tab	"Run another program first"	On/Off	Allows users to specify pre-requisite packages or programs.
	"Run this other program every time"	On/Off	Specifies that the pre-requisite program is run each time the package is run.
Packages>Package> Data Source Tab	"This package contains source files"	On/Off	Determines whether the package contains the source files for the installation.

Location of Option	SMS Option	Setting	Comment
	"Update distribution points on a schedule"	On/Off	Optional setting – used if source files for a package are changed regularly, a schedule for the update may be specified.
Packages>Package> Data Access	"Access distribution folder through common SMS package share"	On/Off	Specifies that the package is accessed from the local machine.
	"Share distribution folder"	<variable>	Optional setting – use if you wish the package to be stored on a remote distribution point.
Advertisements> Schedule tab	"Mandatory Assignments"	<variable>	Optional setting – configures if the user is able to deploy package or not.
	"Allow users to run the program independently of assignments"	On/Off	Optional setting – configures if a user can install a program from Add/Remove Programs.
	"Advertisement will expire"	<variable>	Optional setting – configures if the advertisement is available for a limited period.
Advertisement> Advanced Client tab	"Run program from distribution point"	On/Off	Configures the location from where the package will be installed..
	"Download program from distribution point"	On/Off	Configures the program to be copied locally before it is installed.

Deployment of Executable Files

The following procedure will deploy the Workshare Protect executable with the following settings configured:

- No user interaction.
- The executable is configured to run from a network location and not the client machine.
- The installation will be mandatory and will run with or without a user's permission.

The steps below assume that the pre-requisites for Workshare Protect are already installed.

To deploy the Workshare Protect executable using SMS:

1. Launch the SMS Server Administration Console.
2. Expand the **Site Database** node.

3. Right click the **Packages** node and select **New** and then **Package**. The *Package Properties* dialog is displayed with the **General** tab selected.
4. Specify a **Name** for the package.
5. Optional - specify the **Version** of the package.
6. Optional - specify the **Publisher** of the package.
7. Optional – specify the **Language** of the package.
8. Optional – enter a **Comment**.
9. Select the **Data Source** tab.
10. Select the **This package contains source files** checkbox.
11. Click the **Set…** button. The *Set Source Directory* dialog is displayed.
12. Select the **Local drive on site server** radio button and click **Browse…**. The *Browse for Folder* dialog is displayed.
13. Select the source directory and click **OK**.
14. Click **OK** in the *Set Source Directory* dialog.
15. Select the **Data Access** tab.
16. Verify that the **Access distribution folder through common SMS package share** radio button is selected.
17. Click **OK** in the *Package Properties* dialog.
18. Expand the **<Package Name>** node.
19. Right-click the **Programs** node and select **New** and then **Program**. The *Program Properties* dialog is displayed with the General tab selected.
20. Specify a **Name** for the program.
21. Optional – enter a **Comment**.
22. Click **Browse…**. The *Open* dialog is displayed.
23. Browse to the location of the Workshare install, select the executable and click **Open**. In the **Command Line** field, add the required parameters to configure the install of Workshare Protect. Refer to page *Deploying Workshare Protect with the Self-Extracting Executable*, page 73, for more information. In this example, -product "Workshare Protect" –silent would be required.
24. Select the **Requirements** tab.
25. Optional – specify a value for the **Estimated disk space**.
26. Optional – specify a value for the **Maximum allowed run time**.
27. Optional – select the **This program can run only on specified client platforms** radio button and specify the necessary platform(s) in the field below.
28. Select the **Environment** tab.

29. Select the **Run with administrative rights** radio button.

30. Optional – select the **Allow users to interact with this program** checkbox. This setting configures whether the application is installed silently.

31. Select the **Advanced** tab.

32. Optional – select the **Run another program first** checkbox.

33. Optional – select the necessary "package" or "program" from the dropdown fields. This setting can be used to install pre-requisites.

34. Optional – select the **Run this program every time** checkbox if you wish that the pre-requisite package or program be run each time a package is run.

35. Select **OK** in the *Program Properties* dialog.

36. Right-click the **Access Accounts** node and select **New** and then **Windows User Access Account.** The *Access Account Properties* dialog is displayed.

37. Click **Set**. The *Windows User Account* dialog is displayed.

38. Specify the domain user account and click **OK.**

39. In the *Access Account Properties* dialog change the value of the **Permissions** dropdown to **Full Control** and click **OK.**

40. Right-click the **Distribution Points** node and select **New** and then **Distribution Point**. The *New Distribution Points Wizard* is displayed.

41. Select the **Don't show this page in future** checkbox and click **Next>**. The *Copy Package* dialog is displayed.

42. Select the required distribution point and click **Finish.**

43. Right click the **Advertisements** node and select **New** and then **Advertisement**. The *Advertisement Properties* dialog is displayed.

44. Specify a value for the **Name**.

45. Optional – specify a **Comment.**

46. Select a package from the **Package** dropdown.

47. Select a program from the **Program** dropdown.

48. Click **Browse….** The *Browse Collection* dialog is displayed.

49. Select the required collection and click **OK.**

50. Select the **Schedule** tab.

51. Select the * button to generate a mandatory assignment. The *Assignment Schedule* dialog is displayed.

52. Select the **Assign immediately after this event** radio button.

53. Ensure that **As soon as possible** is displayed in the dropdown and click **OK.**

54. Select the **Advanced Client** tab.

55. Optional – select the **Download Program from distribution point** button.

56. Click **OK** in the *Advertisement Properties* dialog.

The Workshare.InstallWizard.exe may also be specified at Step 13 as the "program" for deployment. If deploying Workshare Protect in this way, ensure that the contents of the self-extracting WorkshareProtect-9800.XXX.exe are all stored at the same location as the Install Wizard.

Deployment of Applications Using MSI Files

The following procedure will deploy Workshare Protect using the msi with the following settings configured:

- User interaction.
- The executable is configured to run from the client machine.
- The installation will be optional.

To deploy the Workshare Protect msi using SMS:

1. Launch the SMS Administrator Console.
2. Launch the SMS Server Administration Console.
3. Expand the **Site Database** node.
4. Right click the **Packages** node and select **New** and then **Package**. The *Package Properties* dialog is displayed with the **General** tab selected.
5. Specify a **Name** for the package.
6. Optional - specify the **Version** of the package.
7. Optional - specify the **Publisher** of the package.
8. Optional – specify the **Language** of the package.
9. Optional – enter a **Comment**.
10. Select the **Data Source** tab.
11. Select the **This package contains source files** checkbox.
12. Select the **Set…** button. The *Set Source Directory* dialog is displayed.
13. Select the **Local drive on site server** radio button and click **Browse**. The *Browse for Folder* dialog is displayed.
14. Select the source directory and click **OK**. The *Set Source Directory* dialog is displayed.
15. Click **OK**.
16. Select the **Data Access** tab. Verify that the **Access distribution folder through common SMS package share** radio button is selected.
17. Select **OK** in the *Package Properties* dialog.
18. Expand the **<Package Name>** node.

19. Right-click the **Programs** node and select **New** and then **Program**.

20. Specify a **Name** for the program.

21. Optional – enter a **Comment**.

22. Select **Browse…** . The *Open* dialog is displayed.

23. Select the **WorksharePdfConverter.msi** and click **OK**.

24. In the **Command Line** field of the *Program Properties* dialog, add the required parameters to configure the installation of Workshare Protect. Refer to *Installation Procedure Using the MSI Files Directly*, page 74, for more information. In this example, /qn would be required.

25. Select the **Environment** tab.

26. Select the **Run with administrative rights** radio button.

27. Click **OK**.

28. Right-click the **Programs** node and select **New** and then **Program**.

29. Specify a **Name** for the program.

30. Optional – enter a **Comment**.

31. Click **Browse…**. The *Open* dialog is displayed.

32. Select the **WorkshareProtect.msi** (change the **Files of Type** filter to **All Files (*.*)** to view the file) and click **OK**.

33. In the **Command Line** field in the *Program Properties* dialog append to the existing text the msi parameters necessary to deploy the **WorkshareProtect.msi**. Consult the *Workshare Protect Installation Guide* for more information.

34. Select the **Environment** tab.

35. Select the **Run with administrative rights** radio button.

36. Select the **Advanced** tab.

37. Select the **Run another program first** checkbox.

38. From the **Package** dropdown select the package that contains the **WorksharePdfConverter.msi** program.

39. From the **Program** dropdown select the disabled features program.

40. Select the **Run this other program every time** checkbox.

41. Right-click the **Access Accounts** node and select **New** and then **Windows User Access Account**. The *Access Account Properties* dialog is displayed.

42. Click **Set**. The *Windows User Account* dialog is displayed.

43. Specify the domain user account and click **OK**.

44. In the *Access Account Properties* dialog change the value of the **Permissions** dropdown to **Full Control** and click **OK**.

45. Right-click the **Distribution Points** node and select **New** and then **Distribution Point**. The *New Distribution Points Wizard* is displayed.

46. Select the **Don't show this page in future** checkbox and click **Next>**. The *Copy Package* dialog is displayed.

47. Select the required distribution point and click **Finish**.

48. Right click the **Advertisements** node and select **New** and then **Advertisement**. The *Advertisement Properties* dialog is displayed.

49. Specify a value for the **Name**.

50. Optional – specify a **Comment>**.

51. Select a package from the **Package** dropdown.

52. Select **Workshare** from the **Program** dropdown. This is to ensure that Workshare is installed – the ordering of the programs will ensure that the programs are installed in the correct order.

53. Click **Browse…**. The *Browse Collection* dialog is displayed.

54. Select the required collection and click **OK**.

55. Select the **Advanced Client** tab.

56. Select the **Download program from the distribution point** radio button.

57. Click **OK**.

The package will be advertised to the members of the selected collection and may be installed from Add/Remove Programs.

Glossary

Term	Definition
Server Locator Point	An SMS 2003 site system that locates CAPs and management points for SMS clients.
DDR	(Discovery Data Record) The file format and the actual file that reports discovery to an SMS site database.
Distribution Point	A site system that has the distribution point role and stores package source files. Clients contact distribution points to obtain source files when they run programs that are advertised to them through a client access point or management point.
Client Agent	Software that runs on SMS clients to perform specific functions. For example, the Software Metering Client Agent reports the applications that ran on the client to the site.
Management Point	The SMS site system that serves as the primary point of contact between the Advanced Clients and the SMS site server.
Package	An object that contains the files and instructions for distributing software to a distribution point and executing the package on SMS clients targeted by advertisements.

Advertisement Program	A program that has been advertised to a collection, but that the clients are not required to run.
Collection	A set of resources in a site. The set is defined by membership rules. Collections are used to distribute software, view the inventories of clients, and access clients for remote control of sessions. An example of a collection is “All Windows NT 4.0 Systems”.
Assigning	In Windows 2000, Windows XP, the Windows Server 2003 family, and systems Management Server (SMS), to deploy a program to members of a group, where installation of the program is mandatory.

Appendix A. Additional Msiexec.exe Parameters and Switches

The executable program that interprets packages and installs products is msiexec.exe. Note that msiexec also sets an error level on return that corresponds to system error codes. The following table describes the parameters and switches for this program. For the latest Msiexec.exe Parameters and Switches, please refer to http://msdn2.microsoft.com/en-us/library/aa367988.aspx.

Switch	Parameters	Meaning
/i	Package|ProductCode	Installs or configures a product.
/f	[p|o|e|d|c|a|u|m|s|v] Package|ProductCode	Repairs a product. This option ignores any property values entered on the command line. The default argument list for this option is 'pecms'. This option shares the same argument list as the REINSTALLMODE property. p Reinstall only if file is missing. o Reinstall if file is missing or if an older version is installed. e Reinstall if file is missing or an equal or older version is installed. d Reinstall if file is missing or a different version is installed. c Reinstall if file is missing or the stored checksum does not match the calculated value. Only repairs files that have msidbFileAttributesChecksum in the Attributes column of the File table. a Force all files to be reinstalled. u Rewrite all required user specific Registry entries. m Rewrite all required computer-specific Registry entries. s Overwrite all existing shortcuts. v Run from source and re-cache the local package. Do not use the v reinstall option for the first installation of an application or feature.
/a	Package	Administrative installation option. Installs a product on the network.
/x	Package|ProductCode	Uninstalls a product.

Switch	Parameters	Meaning
/j	[u|m]Package or [u|m]Package /t Transform List or [u|m]Package /g LanguageID	Advertises a product. This option ignores any property values entered on the command line. u Advertise to the current user. m Advertise to all users of machine. g Language identification. t Applies transform to advertised package.
/L	[i|w|e|a|r|u|c|m|o|p|v|+|!]Logfile	Specifies path to log file and the flags indicate which information to log. i Status messages w Non-fatal warnings e All error messages a Start up of actions r Action-specific records u User requests c Initial UI parameters m Out-of-memory or fatal exit information o Out-of-disk-space messages p Terminal properties v Verbose output + Append to existing file ! Flush each line to the log "*" Wildcard, log all information except for the v option. To include the v option, specify "/l*v".

Switch	Parameters	Meaning
/m	filename	Generates an SMS status .mif file. Must be used with the install (-i), remove (-x), administrative installation (-a), or reinstall (-f) options. The ISMIF32.DLL is installed as part of the SMS and must be on the path. The fields of the status mif file are filled with the following information: Manufacturer - Author Product - Revision Number Version - Subject Locale - Template Serial Number - not set Installation - set by ISMIF32.DLL to "DateTime" InstallStatus - "Success" or "Failed" Description - Error messages in the following order: 1) Error messages generated by installer. 2) Resource from Msi.dll if install could not commence or user exit. 3) System error message file. 4) Formatted message: "Installer error %i", where %i is error returned from Msi.dll
/p	PatchPackage	Applies a patch. To apply a patch to an installed administrative image you must combine options as follows: /p <PatchPackage> /a <Package>
/q	n|b|r|f	Sets user interface level. q No UI qn No UI qb Basic UI. Use qb! to hide the Cancel button. qr Reduced UI with no modal dialog displayed at the end of the installation. qf Full UI and any authored FatalError, UserExit, or Exit modal dialoges at the end. qn+ No UI except for a modal dialog displayed at the end. qb+ Basic UI with a modal dialog displayed at the end. The modal box is not displayed if the user cancels the installation. Use qb+! or qb!+ to hide the Cancel button. qb- Basic UI with no modal dialoges. Please note that /qb+- is not a supported UI level. Use qb-! or qb!- to hide the Cancel button. Note that the ! option is available with Windows Installer version 2.0 and works only with basic UI. It is not valid with full UI.
/? or /h		Displays copyright information for the Windows Installer.

Switch	Parameters	Meaning
/y	Module	Calls the system API DllRegisterServer to self-register modules passed in on the command line. For example, msiexec /y my_file.dll. This option is only used for Registry information that cannot be added using the Registry tables of the MSI file.
/z	Module	Calls the system API DllUnRegisterServer to unregister modules passed in on the command line. For example, msiexec /z my_file.dll. This option is only used for Registry information that cannot be removed using the Registry tables of the MSI file.

The options /i, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, /p, /y and /z should not be used together. The one exception to this rule is that patching an administrative installation requires using both /p and /a. The options /t and /g should only be used with /j. The options /l and /q can be used with /i, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, and /p.

Appendix B. Integrated Diagnostics

This appendix describes the integrated diagnostics tool in Workshare Protect.

Advanced Diagnostic Tool

Workshare Protect is produced and tested to the highest standards to ensure optimum levels of service for all our customers. In the unlikely event of customers experiencing problems with this product, Workshare Protect is integrated with Advanced Diagnostic Tool (ADT). This tool is designed to assist Workshare Technical Support to gather the information required to diagnose and rapidly resolve your issue.

This software tool is deactivated during the normal running of Workshare Protect and will only be activated when you receive assistance from your Technical Support team. When activated, ADT records the customer's specific environment (operating system, version of Microsoft Office and other applications) and the series of events that lead to the issue arising.

When the ADT is activated, the following icon will appear in your system tray: . When the ADT is running, this icon will animate and appear to rotate.

It is not recommended to use this software without prior discussion with the Technical Support team. Your Technical Support representative will provide full details on how to activate this tool.

Note: *When activated, the ADT records screen activity. Users should avoid viewing or typing sensitive information when it is in use. However, when deactivated, the ADT does not record any user actions.*

Appendix C. Default Policy Set

The installation of Workshare Protect installs a default security policy called **Professional5.policy** at the following location: Documents and Settings/All Users/Application Data/Workshare/Workshare/. The same policy can also be found in a user's local folder as follows: Documents and Settings/[current user]/My Documents/My Policies. When a new user logs in, the default policy is copied to their My Policies folder.

Additionally, a copy of this policy is created in a file called **Professional5.runtimepolicy** at the following location: Documents and Settings/All Users/Application Data/Workshare/Protect Enterprise/PolicySets. It is actually the runtimepolicy file that Workshare Protect applies as the policy set.

A user can change the policy set by modifying the parameters in the Workshare Policy Configuration Manager. Any changes made there update the following files: **Options.xml**, **Professional5.policy** (in the user's My Policies folder) and **Professional5.runtimepolicy**.

The default policy set includes the following policies:

Document Conversion Policy

This policy converts Microsoft Office files to PDF when they are emailed.

This policy includes the following expression:

- File type is Word, Excel, PowerPoint or RTF.

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to Internal: PDF; Everyone to External: PDF (meaning the document is converted to PDF when emailed to an external or an internal recipient)

Hidden Data Policy

This content security policy prevents the unauthorized disclosure of hidden data such as track changes, speaker notes and hidden columns. Depending on the type of hidden data and user privilege, the data is either automatically removed or the user is given the choice to clean the data or disregard the alert.

This policy includes the following expressions:

- Any document (Microsoft Word, Excel or PowerPoint, or PDF) contains high risk hidden data (comment, track change item, hidden text, small text, white text, version, auto version, link, speaker notes, hidden slides), or
- Any document contains medium risk hidden data (reviewer, routing slip, variable, macro, custom property, link), or
- Any document contains low risk hidden data (attached template, field, built-in property, document statistic)

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to External: Clean Hidden Data (meaning when the document is emailed to an external recipient, the hidden data is removed from the document)

- Active Content Channel Action: Active Task Bar (meaning when the document is open, a real-time policy alert is displayed in the bottom right of the screen notifying the user of the policy breach)

Full Document Restriction Policy

This policy prevents documents that have the Workshare classification “full document restriction” from being emailed.

This policy includes the following expressions:

- Any file type has a Workshare ‘Full Restriction’ status.
- Custom property ‘WSClassification’ is ‘Full Restriction’

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to Internal: Block; Everyone to External: Block (meaning the document cannot be emailed to an external or an internal recipient)

External Document Restriction Policy

This policy prevents documents that have the Workshare classification “external document restriction” from being emailed externally.

This policy includes the following expressions:

- Any file type has a Workshare ‘External Only Restriction’ status.
- Custom property ‘WSClassification’ is ‘External Only Restriction’

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to External: Block (meaning the document cannot be emailed to an external recipient)

For Internal Use Only Policy

This policy prevents documents that have the Workshare classification “for internal use only” from being emailed externally.

This policy includes the following expression:

- Custom property ‘WSClassification’ is ‘For Internal Use Only’

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to External: Block (meaning the document cannot be emailed to an external recipient)

Confidential Policy

This policy alerts users when documents that have the Workshare classification “confidential” are emailed.

This policy includes the following expressions:

- Custom property ‘WSClassification’ is ‘Confidential’

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to Internal: Alert; Everyone to External: Alert (meaning when the document is emailed to an external or an internal recipient, the user is alerted)

Highly Confidential Policy

This policy prevents documents that have the Workshare classification “highly confidential” from being emailed.

This policy includes the following expressions:

- Custom property ‘WSClassification’ is ‘Highly Confidential’

The actions to apply when the condition is met are as follows:

- Email Channel Action: Everyone to Internal: Block; Everyone to External: Block (meaning the document cannot be emailed to an external or an internal recipient)

Appendix D. Workshare Protect Prerequisites

Summary

The prerequisites for Workshare Protect 5.2 SR3 depend on the version of the operating system and the version of Microsoft Office. They are listed on page 15 and further details provided in this appendix. Prerequisites for other versions of Workshare Protect may be slightly different.

Windows Installer

Summary

Windows Installer 3.1 is required to allow patching of the product.

Checks

Checker	File	Check
Workshare Install Wizard	%windir%\system32\msi.dll	File is 3.1.0.1 or above
WorkshareProtect.msi		No check is made.

Install Files

OS	Installer
Windows XP	http://download.microsoft.com/download/1/4/7/147ded26-931c-4daf-9095-ec7baf996f46/WindowsInstaller-KB893803-v2-x86.exe
Windows XP x64	http://download.microsoft.com/download/4/8/5/4852c63a-cf27-4e83-baad-47b8372e9e9b/WindowsXP-KB898715-x64-enu.exe
Windows Server 2003	http://download.microsoft.com/download/4/8/5/4852c63a-cf27-4e83-baad-47b8372e9e9b/WindowsServer2003-KB898715-x86-enu.exe
Windows Server 2003 x64	http://download.microsoft.com/download/4/8/5/4852c63a-cf27-4e83-baad-47b8372e9e9b/WindowsServer2003-KB898715-x64-enu.exe
Windows Vista and above	The required version of Windows Installer is distributed with the OS.

Microsoft .NET Framework 3.0

Summary

Microsoft .NET Framework 3.0 (no service pack) includes other installs such as Microsoft .NET Framework 2.0 and MSXML 6.0 which are installed as part of the Framework.

Checks

Checker	Registry Key	Check
Workshare InstallWizard	HKLM\Software\Microsoft\NET Framework Setup\NDP\v3.0\Setup	Value InstallSuccess=1 (DWORD)
WorkshareProtect.msi	HKLM\Software\Microsoft\NET Framework Setup\NDP\v3.0\Setup	Value InstallSuccess exists

Install Files

OS	Installer
x86	http://go.microsoft.com/fwlink/?LinkId=70848
x64	http://go.microsoft.com/fwlink/?LinkId=70849
Windows Vista and above	The required version of Microsoft .NET is distributed with the OS.

KB908002 – Shared Add-in Support Update for Microsoft .NET Framework 2.0

Summary

This update is required for any version of Office to be able to load .NET addins. It is bundled with the Workshare install. You can extract the Office update (lockbackregkey.msi) from the Visual Studio update http://download.microsoft.com/download/b/6/7/b6711d3b-b509-4567-8599-98bf3473310f/vs2005-kb908002-enu-x86.exe.

Checks

Checker	Reg Key	Check
Workshare Install Wizard	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{64F3B15C-24C7-4B2B-9B72-65CCBBD7F06B}	Value DisplayName exists
WorkshareProtect.msi	HKCR\Interface\\{000C0601-0000-0000-C000-000000000046}	Key exists

Install Files

Office	Installer
All versions of Office	lockbackregkey.msi is bundled with the install.

MSXML 6.0

Summary

MSXML 6.0 is bundled and installed with Microsoft .NET Framework 3. Installation of this prerequisite is verified because there have been issues with it in the past.

Checks

Checker	File	Check
WorkshareProtect.msi	%windir%\system32\msxml6.dll	File exists

Install Files

This prerequisite is bundled with Microsoft .NET 3. It is also possible to download it separately from Microsoft.

Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x86)

Summary

Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x86) is required.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{837B34E3-7C30-493C-8F6A-2B0F04E2912C}	Value DisplayName exists
WorkshareProtect.msi	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{837B34E3-7C30-493C-8F6A-2B0F04E2912C}	Value DisplayName exists

Install Files

OS	File
All versions	http://download.microsoft.com/download/6/B/B/6BB661D6-A8AE-4819-B79F-236472F6070C/vcredist_x86.exe

Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x64)

Summary

Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update (x64) is required for the native x64 code in the application.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{071c9b48-7c32-4621-a0ac-3f809523288f}	DisplayName exists
WorkshareProtect.msi	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{071c9b48-7c32-4621-a0ac-3f809523288f}	DisplayName exists

Install Files

OS	File
All 64 bit versions	http://download.microsoft.com/download/6/B/B/6BB661D6-A8AE-4819-B79F-236472F6070C/vcredist_x64.exe

Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x86)

Summary

Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x86) is required.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1F1C2DFC-2D24-3E06-BCB8-725134ADF989}	Value DisplayName exists
WorkshareProtect.msi	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1F1C2DFC-2D24-3E06-BCB8-725134ADF989}	Value DisplayName exists

Install Files

OS	File
All versions	http://download.microsoft.com/download/9/7/7/977B481A-7BA6-4E30-AC40-ED51EB2028F2/vcredist_x86.exe

Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x64)

Summary

Microsoft Visual C++ 2008 SP1 Redistributable Package ATL Security Update (x64) is required for the native x64 code in the application.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4B6C7001-C7D6-3710-913E-5BC23FCE91E6}	DisplayName exists
WorkshareProtect.msi	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{4B6C7001-C7D6-3710-913E-5BC23FCE91E6}	DisplayName exists

Install Files

OS	File
All 64 bit versions	http://download.microsoft.com/download/9/7/7/977B481A-7BA6-4E30-AC40-ED51EB2028F2/vcredist_x64.exe

Microsoft Report Viewer (x86)

Summary

The Microsoft Report Viewer is used to display risk reports. It requires Microsoft .NET Framework 3 to be installed.

The Workshare Install Wizard uses ReportViewerChk.exe to determine if the report viewer is installed. ReportViewerChk.exe is bundled with the Protect 5.2 SR3 install and initially came from the Visual Studio 2005 install.

Checks

Checker	File / Registry Key	Check
Workshare Install Wizard	Uses the bundled exe ReportViewerChk.exe	ReportViewerChk.exe returns 1
WorkshareProtect.msi	HKLM\Software\Microsoft\ReportViewer\v2.0.50727	Value Install exists

Install Files

OS	File
All versions	http://download.microsoft.com/download/2/7/f/27faefe6-1a8b-4d05-a8cf-abd8043268a9/ReportViewer.exe

KB907417 – Update for Office 2003

Summary

The KB907417 Update for Office 2003 enables Microsoft Word 2003 and Microsoft Excel 2003 to load .NET addins.

Checks

Checker	File	Check
Workshare Install Wizard	[OFFICE2003_PATH]\Addins\OTKLOADR.DLL	File version is 7.10.5077.0 or greater
WorkshareProtect.msi	[OFFICE2003_PATH]\Addins\OTKLOADR.DLL	File version is 7.10.5077.0 or greater

Install Files

Office Version	File
Office 2003	http://download.microsoft.com/download/5/a/6/5a6c111a-4392-41dc-a1b3-87ea0083950a/office2003-KB907417-FullFile-ENU.exe

KB935514 – Update for Office 2007

Summary

The KB935514 Update for Office 2007 is required for Office 2007 (no service pack). This update has been included in Office 2007 service pack 1.

Checks

Checker	File / Registry Key	Check
Workshare Install Wizard	[OFFICE2007_PATH]\WWLIB.DLL	File version is 12.0.6016.5000 or greater
WorkshareProtect.msi	[OFFICE2007_PATH]\WWLIB.DLL	File version is 12.0.6016.5000 or later

Install Files

Office Version	File
Office 2007	http://download.microsoft.com/download/8/2/4/8242897a-5aef-4ffa-bfb0-02a25c26fd01/office-kb935514-fullfile-x86-glb.exe

Microsoft Office System Primary Interop Assemblies (PIA)

Summary

The Microsoft Office System Primary Interop Assemblies are used by .NET programs to communicate with Office.

You can extract the Office PIAs (o2007pia.msi) from the Office download http://download.microsoft.com /download/e/1/d/e1df4622-5f6c-4fb9-845b-38d009cc1188/PrimaryInteropAssembly.exe.

Checks

Checker	File / Registry Key	Check
Workshare Install Wizard	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{50120000-1105-0000-0000-0000000FF1CE}	Value DisplayName exists
WorkshareProtect.msi		No check is made.

Install Files

Office Version	File
Office 2007	o2007pia.msi can be extracted from http://download.microsoft.com/download/e/1/d/e1df4622-5f6c-4fb9-845b-38d009cc1188/PrimaryInteropAssembly.exe.

Open XML Format SDK

Summary

This prerequisite is required to be able to read and write Microsoft Office XML files. It is bundled with the Workshare install. You can download the installer from http://download.microsoft.com/download/7/7/3/7737344c-40f6-47f3-9f5e-be8e7a7a0a89/OpenXMLSDK.msi.

Checks

Checker	Reg Key	Check
Workshare Install Wizard	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F565EF2B-9A5C-49EB-BEE1-7FAF8E998330}	Value DisplayName exists
WorkshareProtect.msi		No check is made.

Install Files

OS	Installer
All versions	http://download.microsoft.com/download/7/7/3/7737344c-40f6-47f3-9f5e-be8e7a7a0a89/OpenXMLSDK.msi

KB898715 - Windows Installer for Server 2003 (x64)

Summary

KB898715 - Windows Installer for Server 2003 (x64) is required for patching.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	%windir%\system32\msi.dll	File is 3.1.0.1 or above
WorkshareProtect.msi		No check is made.

Install Files

OS	File
Windows Server 2003 x64	http://download.microsoft.com/download/4/8/5/4852c63a-cf27-4e83-baad-47b8372e9e9b/WindowsServer2003-KB898715-x64-enu.exe

KB898715 - Windows Installer for Server 2003 (x86)

Summary

KB898715 - Windows Installer for Server 2003 (x86) is required for patching.

Checks

Checker	Registry Key	Check
Workshare Install Wizard	%windir%\system32\msi.dll	File is 3.1.0.1 or above
WorkshareProtect.msi		No check is made.

Install Files

OS	File
Windows Server 2003 x86	http://download.microsoft.com/download/4/8/5/4852c63a-cf27-4e83-baad-47b8372e9e9b/WindowsServer2003-KB898715-x86-enu.exe