

User Manual

Foxit[®] PDF Secure RMS Protector



Gold Independent Software Vendor (ISV)

© Foxit Software Incorporated. All rights reserved.

Copyright © Foxit Software Incorporated. All Rights Reserved.

No part of this document can be reproduced, transferred, distributed or stored in any format without the prior written permission of Foxit.

Anti-Grain Geometry - Version 1.1

Copyright (C) 2002-2005 Maxim Shemanarev (http://www.antigrain.com)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Contents

Chapter 1 - Overview	5
Chapter 2 - For SharePoint	6
Getting Started	6
System Requirements	6
Corresponding permissions of Foxit Reader and MOSS	7
Installing Foxit PDF Secure RMS Protector on a SharePoint Server	8
View and Manage Event Logs of Foxit PDF Secure RMS Protector	14
Check the version of Foxit PDF Secure RMS Protector	16
Editing Wrapper Content	17
Configuring AD RMS to Work with SPS-SRV	
For MOSS 2007	
To add SPS-SRV to Local Intranet	17
To add SPS-SRV to the AD·RMS Certification Pipeline	18
To activate Information Rights Management in Office SharePoint Server 2007	18
To restrict permissions using AD·RMS	18
For MOSS 2010	19
To add SPS-SRV to Local Intranet	19
To add SPS-SRV to the AD·RMS Certification Pipeline	19
To activate Information Rights Management in Office SharePoint Server 2010	
To restrict permissions using AD·RMS	20
For MOSS 2013 and 2016	20
To add SPS-SRV to Local Intranet	20
To add SPS-SRV to the AD·RMS Certification Pipeline	21
To activate Information Rights Management in Office SharePoint Server 2013 a	and
2016	
To restrict permissions using AD·RMS	
Working with Foxit PDF Secure RMS Protector	
For MOSS 2007	
To add the domain user to SharePoint site	
To set the group permission in SharePoint site	
To restrict the print permissions using RMS	
For MOSS 2010	
To add the domain user to SharePoint site	
To set group permission in SharePoint site	
To restrict the print permissions using RMS	
For MOSS 2013 and 2016	32

To add the domain user to SharePoint site	32
To set group permission in SharePoint site	33
To restrict the print permissions using RMS	35
Chapter 3 - For Exchange	37
Getting Started	37
System Requirements	37
Corresponding permissions of Foxit Reader and Exchange	38
Installing Foxit PDF Secure RMS Protector on an Exchange Server	38
Uninstalling Foxit PDF Secure RMS Protector	41
Check the version of Foxit PDF Secure RMS Protector	43
Editing Wrapper Content	44
Configuring AD·RMS to Integrate with Exchange Server in a Single Forest	44
To register a service connection point	45
To give Exchange servers permissions to access the server certification pipeline	45
To set up the Exchange Server super users group	46
To set InternalLicensingEnable true by ExchangeManagement Shell	46
Working with Foxit PDF Secure RMS Protector	47
For Exchange 2010	47
For Exchange 2013 and 2016	50
Chapter 4 - Watermark Configuration Tool	53
Creating Profile	53
Adding Watermark	54
Editing or Deleting Watermark	55
Importing or Exporting Watermark	55
Chapter 5 - FAQ	
Contact Us	58

Chapter 1 - Overview

Traditionally, sensitive information can only be controlled by limiting access to the networks or computers where the information is stored. After access is given to users, however, there are no restrictions on what can be done with the content or to whom it can be sent. Microsoft Information Rights Management (IRM) enables you to create a persistent set of access controls that live with the content, rather than a specific network location, which will help you control access to files even after they leave your direct control.

Foxit PDF Secure RMS protector extends all the benefits of AD RMS to any PDF document. In addition, Foxit PDF Secure RMS protector provides creation and control of rights to unique PDF features.

Microsoft's Active Directory Rights Management (AD·RMS) solves security problems for enterprise documents created in Microsoft Office. With the inclusion of AD RMS in Windows Server2008, AD RMS has quickly become the default standard for document rights protection.

For the enterprises, they can enforce security policies easily to protect sensitive information, as well as enable each PDF document with additional features such as forms fill out and annotations.

Chapter 2 - For SharePoint

4 Getting Started

This section provides system requirements, install and uninstall instructions for the RMS Protector.

System Requirements

System Requirements for MOSS 2007

Computer	Operating System	Requirement
RMS Server/ ADRMS	Windows Server-2003	RMS, Internet Information Services
Server	with Service Pack·1	(IIS) 6.0, World Wide Web Publishing
	(SP1)/Windows	Service, Message Queuing (also
	Server·2008 with Service	known as MSMQ), and Microsoft
	Pack·1 (SP1)	SQL Server™·2005 Standard Edition
DC	Windows Server-2003	Active Directory, Domain Name
	with SP1	System (DNS)
ADRMS-DB	Windows·Server·2003	Microsoft SQL Server™·2005 with
	with SP1	Service Pack·2 (SP2)
SharePoint Server	Windows Server-2003	Office SharePoint Server-2007 with
Such as named SPS-SRV	with SP1	RMS Client installed, and has been
		added this Server to DC

System Requirements for MOSS 2010

Computer	Operating S	ystem	Requirement
ADRMS Server	Windows	Server·2008	RMS, Internet Information Services
	with Service	e Pack·1 (SP1)	(IIS) 6.0, World Wide Web Publishing
			Service, Message Queuing (also
			known as MSMQ)
DC	Windows	Server·2003	Active Directory, Domain Name
	with SP1		System (DNS)
ADRMS-DB	Windows·Se	erver·2008	Microsoft SQL Server™·2008 R2
	with SP1		
SharePoint Server	Windows	Server·2008	Office SharePoint Server-2010 and
Such as named SPS-SRV	with SP2		has been added this Server to DC

System Requirements for MOSS 2013

Computer	Operating S	ystem	Requirement
ADRMS Server	Windows	Server·2008	RMS, Internet Information Services
	with Service	e Pack·1 (SP2)	(IIS) 6.0, World Wide Web Publishing
			Service, Message Queuing (also
			known as MSMQ)
DC	Windows	Server·2008	Active Directory, Domain Name
	with SP2		System (DNS)
ADRMS-DB	Windows·Se	erver·2008	Microsoft SQL Server™·2008 R2
	with SP1		
SharePoint Server	Windows Se	erver·2012	Office SharePoint Server-2013 and
Such as named SPS-SRV			has been added this Server to DC

System Requirements for MOSS 2016

Computer	Operating System	Requirement
ADRMS Server	Windows Server · 2012	RMS, Internet Information Services
		(IIS)
DC	Windows Server · 2012	Active Directory, Domain Name
		System (DNS)
ADRMS-DB	Windows·Server·2012	Microsoft SQL Server™·2012
SharePoint Server	Windows Server 2012	Office SharePoint Server-2016 and
Such as named SPS-SRV		has been added this Server to DC

Corresponding permissions of Foxit Reader and MOSS

SharePoint service provides three levels rights: Full control, Change, and Read.

Level	Rights of Foxit Reader
Full control	View, Copy, Modify, Print, View Data, Access, Annotate, Fill Form,
	Assemble
Change	View, Copy, Modify, Access, Annotate, Fill Form, Assemble
Read	View

The user only can print the document if its library IRM settings have been configured to allow document printing.

Installing Foxit PDF Secure RMS Protector on a SharePoint Server

To install Foxit PDF Secure RMS Protector:

- Stop the IIS Admin service: Start > Settings > Control Panel > Administrator Tools > Services > IIS Admin Service > Stop. Then Close the window.
- Run the Foxit PDF Secure RMS Protector Setup program to install the protector on the server.



- Download PDF icon from <u>http://www.foxitsoftware.com/resource/images/icons/pd</u> <u>f-icon.png</u>.
- For MOSS 2007
 - 1. Copy the downloaded .png file to "Drive: \Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Template\Images".
 - 2. Edit the file "Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\12\Template\Xml\DOCICON.XML":
 - a. Right-click DOCICON.XML file > click Open With > select Notepad.
 - b. Add an entry for the .pdf extension as the file's name. For example, type the ICPDF as the name of the .png file:

<Mapping Key="pdf" Value="pdf-icon.png"/>

Foxit PDF Secure RMS Protector

User Manual

DOCICON.XML - Note File Edit Format View	
	·
pencontrol= Sna Monning	rePoint.OpenDocuments"/> Key="ODC.Table" Value="icodct.gif" EditText="Microsoft Excel"
<pre>vnapping vnapControl="sha</pre>	repoint.openDocuments"/>
Manning/	Key="Onenote.Notebook" Value="icnotebk.pnq" EditText="Microsoft OneNote"
penControl="Sha	report.OpenDocuments"/>
<mapping< td=""><td>rePoint.OpenDocuments"/> Key="PowerPoint.Slide" Value="ichtmppt.gif" EditText="Microsoft PowerPoint"</td></mapping<>	rePoint.OpenDocuments"/> Key="PowerPoint.Slide" Value="ichtmppt.gif" EditText="Microsoft PowerPoint"
pencontrol="sha	rePoint.OpenDocuments"/>
<mapping< td=""><td>Key="Publisher.Document" Value="ichtmpub.qif" EditText="Microsoft Publisher"</td></mapping<>	Key="Publisher.Document" Value="ichtmpub.qif" EditText="Microsoft Publisher"
	rePoint OpenDocuments"/>
<mapping< td=""><td>Key="SharePoint.DocumentSet" Value="icdocset.gif"/></td></mapping<>	Key="SharePoint.DocumentSet" Value="icdocset.gif"/>
<mapping< td=""><td>Key="SharePoint.webPartPage.Document" Value="icsmrtpg.gif" EditText="Microsoft ner" OpenControl="SharePoint.OpenDocuments"/></td></mapping<>	Key="SharePoint.webPartPage.Document" Value="icsmrtpg.gif" EditText="Microsoft ner" OpenControl="SharePoint.OpenDocuments"/>
SharePoint Desig	ner" OpenControl="SharePoint.OpenDocuments"/>
<mapping< td=""><td><pre>Key="Visio.webDrawing" Value="icvdw.gif" EditText="Microsoft Visio" rePoint.OpenDocuments"/></pre></td></mapping<>	<pre>Key="Visio.webDrawing" Value="icvdw.gif" EditText="Microsoft Visio" rePoint.OpenDocuments"/></pre>
/pencontrol= Sna /Mapping	report.openDocuments />
nenControl-"Sha	Key="Word.Document"
Manning/	Kev="XDocs.Document" Value="icxddoc.gif" EditText="Microsoft InfoPath"
	repoint.OpenXMLDocuments"/>
<mapping< td=""><td>Kev="SharePoint.Link" Value="DOCLINK.GIF"/></td></mapping<>	Kev="SharePoint.Link" Value="DOCLINK.GIF"/>
<mapping< td=""><td>Key="SharePoint.Link" Value="DOCLINK.GIF"/> Key="SharePoint.SearchAdminReport" Value="icsadrep.gif" EditText="Microsoft</td></mapping<>	Key="SharePoint.Link" Value="DOCLINK.GIF"/> Key="SharePoint.SearchAdminReport" Value="icsadrep.gif" EditText="Microsoft
SharePoint Desig	ner" OpenControl="SharePoint.OpenDocuments"/>
<byextension< td=""><td></td></byextension<>	
<mapping< td=""><td><pre>key="pdf" Value="pdf-icon.png"/> key="accdb" value="icaccdb.gif" EditText="Microsoft Access"</pre></td></mapping<>	<pre>key="pdf" Value="pdf-icon.png"/> key="accdb" value="icaccdb.gif" EditText="Microsoft Access"</pre>
<mapping< td=""><td>repoint.OpenDocuments"/></td></mapping<>	repoint.OpenDocuments"/>
/penconcroi= sna Mapping	Key="accdt" Value="icaccdb.gif"/>
<mapping< td=""><td>Key="accdc" Value="icaccdb.gif"/> Key="accdc" Value="icaccdb.gif"/></td></mapping<>	Key="accdc" Value="icaccdb.gif"/> Key="accdc" Value="icaccdb.gif"/>
<mapping< td=""><td>Key="accde" Value="icaccde.gif" EditText="Microsoft Access"</td></mapping<>	Key="accde" Value="icaccde.gif" EditText="Microsoft Access"
penControl="Sha	repoint.OpenDocuments"/>
<mapping< td=""><td>Key="accdr" Value="icaccde.gif" EditText="Microsoft Access"</td></mapping<>	Key="accdr" Value="icaccde.gif" EditText="Microsoft Access"
pen⊂ontrol="Shā	rePoint.OpenDocuments"/>
<mapping< td=""><td>Kev="asax" Value="icasax.gif" OpenControl=""/></td></mapping<>	Kev="asax" Value="icasax.gif" OpenControl=""/>
<mapping< td=""><td>Key="ascx" Value="icascx.gif" EditText="Microsoft SharePoint Designer"</td></mapping<>	Key="ascx" Value="icascx.gif" EditText="Microsoft SharePoint Designer"
penControl="Sha	rePoint.OpenDocuments"/>
<mapping< td=""><td>Key="asmx" Value="icasmx.gif" OpenControl=""/> Key="asp" Value="ichtm.gif" OpenControl=""/></td></mapping<>	Key="asmx" Value="icasmx.gif" OpenControl=""/> Key="asp" Value="ichtm.gif" OpenControl=""/>
<mapping< td=""><td>Key="asp" value="ichtm.gif" OpenControl=""/> Key="aspx" value="ichtm.gif" EditText="Microsoft SharePoint Designer"</td></mapping<>	Key="asp" value="ichtm.gif" OpenControl=""/> Key="aspx" value="ichtm.gif" EditText="Microsoft SharePoint Designer"
<mapping< td=""><td>Rey= aspx value= ichum.gli Eulliext= Microsoft SharePoint Designer</td></mapping<>	Rey= aspx value= ichum.gli Eulliext= Microsoft SharePoint Designer

c. Click Save on the File menu, and then quit Notepad.

• For MOSS 2010

- Copy the downloaded .png file to "Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\Template\Images"
- 2. Edit the file "Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\14\Template\Xml\DOCICON.XML":
 - a. Right-click DOCICON.XML file > click Open With > select Notepad.

b. Add an entry for the .pdf extension as the file's name. For example, type the ICPDF as the name of the .png file:

<Mapping Key="pdf" Value="pdf-icon.png"/>

Foxit PDF Secure RMS Protector

User Manual

_	N.XML - Not Format Viev	· · · · · · · · · · · · · · · · · · ·	
		arePoint.OpenDocuments"/>	
•	<mapping< td=""><td>q Key="ODC.Table" Value="icodct.gif" EditText="Microsoft Excel"</td><td></td></mapping<>	q Key="ODC.Table" Value="icodct.gif" EditText="Microsoft Excel"	
OpenCont	trol="sha	arePoint.OpenDocuments"/>	
	<mapping< td=""><td>g Key="Onenote.Notebook" Value="icnotebk.png" EditText="Microsoft OneNote"</td><td></td></mapping<>	g Key="Onenote.Notebook" Value="icnotebk.png" EditText="Microsoft OneNote"	
opencont	trol="Sha	ărePoint.OpenDocuments"/> g Key="PowerPoint.Slide" Value="ichtmppt.gif" EditText="Microsoft PowerPoint"	
	<mapping< td=""><td>arePoint.openDocuments"/></td><td></td></mapping<>	arePoint.openDocuments"/>	
opencon	ZManning	a erothe.openbocoments // a Kev-"Publisher Document" Value-"ichtmoub dif" EditText-"Microsoft Publisher"	
onenCont	trol="sha	g Key="Publisher.Document" Value="ichtmpub.gif" EditText="Microsoft Publisher" arePoint.OpenDocuments"/>	
	<mapping< td=""><td>g Key="SharePoint.DocumentSet" value="icdocset.gif"/></td><td></td></mapping<>	g Key="SharePoint.DocumentSet" value="icdocset.gif"/>	
	<mapping< td=""><td>g Key="SharePoint.Documentset" Value="icdocset.gif"/> g Key="SharePoint.WebPartPage.Document" Value="icsmrtpg.gif" EditText="Microsoft gner" openControl="SharePoint.openDocuments"/></td><td>: </td></mapping<>	g Key="SharePoint.Documentset" Value="icdocset.gif"/> g Key="SharePoint.WebPartPage.Document" Value="icsmrtpg.gif" EditText="Microsoft gner" openControl="SharePoint.openDocuments"/>	:
SharePoi	int Desig	gner" opencontrol="SharePoint.OpenDocuments"/>	
	<mapping< td=""><td>g Key="Visio.WebDrawing" Value="icvdw.gif" EditText="Microsoft Visio"</td><td></td></mapping<>	g Key="Visio.WebDrawing" Value="icvdw.gif" EditText="Microsoft Visio"	
opencont	trol="Sha	arePoint.openDocuments"/>	
	<mapping< td=""><td>g Key="Word.Document" value="ichtmdoc.gif" EditText="Microsoft Word" arePoint.OpenDocuments"/> g Key="XDocs.Document" Value="icxddoc.gif" EditText="Microsoft InfoPath"</td><td></td></mapping<>	g Key="Word.Document" value="ichtmdoc.gif" EditText="Microsoft Word" arePoint.OpenDocuments"/> g Key="XDocs.Document" Value="icxddoc.gif" EditText="Microsoft InfoPath"	
pencon	<mapping< td=""><td>a Port", Openbocuments //</td><td></td></mapping<>	a Port", Openbocuments //	
onenCont	trol="sha	arePoint.openXMLDocuments"/>	
opencon	<mapping< td=""><td>G Kev="SharePoint.Link" Value="DOCLINK.GIF"/></td><td></td></mapping<>	G Kev="SharePoint.Link" Value="DOCLINK.GIF"/>	
	<mappind< td=""><td>g Key="SharePoint.Link" Value="DOCLINK.GIF"/> g Key="SharePoint.SearChAdminReport" Value="icsadrep.gif" EditText="Microsoft gner" openControl="SharePoint.openDocuments"/></td><td></td></mappind<>	g Key="SharePoint.Link" Value="DOCLINK.GIF"/> g Key="SharePoint.SearChAdminReport" Value="icsadrep.gif" EditText="Microsoft gner" openControl="SharePoint.openDocuments"/>	
SharePoi	int Desig	ğner" OpenControl="SharePoint.OpenDocuments"/>	
	/ProgID>		
<by< td=""><td>Extension</td><td></td><td></td></by<>	Extension		
L	<mapping< td=""><td>g Key="pdf" Value="pdf-icon.png"/> g Key="accdb" Value="icaccdb.gff" EditText="Microsoft Access"</td><td></td></mapping<>	g Key="pdf" Value="pdf-icon.png"/> g Key="accdb" Value="icaccdb.gff" EditText="Microsoft Access"	
	<mapping< td=""><td>arePoint.OpenDocuments"/></td><td></td></mapping<>	arePoint.OpenDocuments"/>	
pencon	<manning< td=""><td>a Ferdina openboline (1977)</td><td></td></manning<>	a Ferdina openboline (1977)	
	<mapping< td=""><td>g Key="accdt" value="icaccdb.gif"/> g Key="accdc" value="icaccdb.gif"/></td><td></td></mapping<>	g Key="accdt" value="icaccdb.gif"/> g Key="accdc" value="icaccdb.gif"/>	
	<mapping< td=""><td>q Kev="accde" Value="icaccde.qif" EditText="Microsoft Access"</td><td></td></mapping<>	q Kev="accde" Value="icaccde.qif" EditText="Microsoft Access"	
penCont	trol'="sha	árePóint OpenDocuments"/>	
-	<mapping< td=""><td>q Key="accdr" Value="icaccde.gif" EditText="Microsoft Access"</td><td></td></mapping<>	q Key="accdr" Value="icaccde.gif" EditText="Microsoft Access"	
opencont	trol="Sha	arePoint.OpenDocuments"/>	
	<mapping< td=""><td>g Key="asax" Value="icasax.gif" OpenControl=""/></td><td></td></mapping<>	g Key="asax" Value="icasax.gif" OpenControl=""/>	
	<mapping< td=""><td>g Key="asax" Value="icasax.gif" OpenControl=""/> g Key="ascx" Value="icascx.gif" EditText="Microsoft SharePoint Designer" arePoint.OpenDocuments"/></td><td></td></mapping<>	g Key="asax" Value="icasax.gif" OpenControl=""/> g Key="ascx" Value="icascx.gif" EditText="Microsoft SharePoint Designer" arePoint.OpenDocuments"/>	
pencont	unot= Sha ∠Mapping	arePoint.openDocuments /> q Key="asmx" Value="icasmx.qif" OpenControl=""/>	
	<mapping ZManning</mapping 	g Key="asm" value="ichtm.gif" OpenControl="/> g Key="asp" value="ichtm.gif" OpenControl=""/>	
	- Manning	g Key="asp" value="ichtm.gif" EditText="Microsoft SharePoint Designer"	

c. Click Save on the File menu, and then quit Notepad.

• For MOSS 2013

- Copy the downloaded .png file to "Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\Template\Images"
- 2. Edit the file "Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\15\Template\Xml\DOCICON.XML":
 - a. Right-click DOCICON.XML file > click Open With > select Notepad.

b. Add an entry for the .pdf extension as the file's name. For example, type the ICPDF as the name of the .png file:

<Mapping Key="pdf" Value="pdf-icon.png"/>

Foxit PDF Secure RMS Protector

User Manual

D O	ICON.XML - Notepad
File E	dit Format View Help
opend	Control="SharePoint.OpenDocuments"/>
	<pre><mapping control="SharePoint.OpenDocuments" edittext="Microsoft Excel" key="ODC.Table" value="icodct.gif"></mapping></pre>
pend	<pre></pre> <pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre> <p< td=""></p<></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
pend	introl="sharepoint.openDocuments"/>
. 1	control="SharePoint.OpenDocuments"/> <mapping <="" edittext="Microsoft PowerPoint" key="PowerPoint.Slide" td="" value="ichtmppt.gif"></mapping>
pend	Control="SharePoint.OpenDocuments"/>
	<pre><mapping <="" edittext="Microsoft Publisher" key="Publisher.Document" pre="" value="ichtmpub.gif"></mapping></pre>
peno	control="SharePoint.OpenDocuments"/> <mapping key="SharePoint.DocumentSet" value="icdocset.gif"></mapping>
	<pre><mapping <="" edittext="Microsoft" focument"="" key="SharePoint" pre="" value="icsmrtng dif" webpartdade=""></mapping></pre>
share	Point Designer" OpenControl="SharePoint.OpenDocuments"/>
	<pre></pre> <pre><</pre>
pend	Control="SharePoint.OpenDocuments"/>
	<pre><mapping <="" edittext="Microsoft word" key="word.Document" pre="" value="ichtmdoc.gif"></mapping></pre>
pend	Iontrol="ShārePóint.OpenDocuments"/> <mapping <="" edittext="Microsoft InfoPath" key="XDocs.Document" td="" value="icxddoc.gif"></mapping>
non	<pre>control="sharePoint.openxMLDocument"/></pre>
pen	<pre>control = print.open/web/content/set/set/set/set/set/set/set/set/set/se</pre>
	<pre><mapping key="SharePoint.Link" value="DOCLINK.GIF"></mapping> <mapping edittext="Microsoft Point Designer" key="SharePoint.SearchAdminReport" opencontrol="SharePoint.OpenDocuments" value="icsadrep.gif"></mapping></pre>
share	ePoint besigner" OpenControl="SharePoint.openDocuments"/>
	(ByExtension>
	<pre></pre> Amapping Key="pdf" value="pdf-icon.png"/> <pre><mapping <="" edittext="Microsoft Access" key="accdb" pre="" value="icaccdb.gif"></mapping></pre>
non	<pre>cmapping key= accob value= reaccob.gr = Entrext= Microsoft Access ontrol = "sharePoint.OpenDocuments"/></pre>
perk	<pre></pre>
	<mapping key="accdc" value="icaccdb.gif"></mapping>
	<pre><mapping key="accdt" value="icaccdb.gif"></mapping> <mapping key="accdc" value="icaccdb.gif"></mapping> <mapping <="" edittext="Microsoft Access" key="accde" pre="" value="icaccde.gif"></mapping></pre>
pend	Control="SharePoint.OpenDocuments"/>
	<pre><mapping control="SharePoint.OpenDocuments" edittext="Microsoft Access" key="accdr" value="icaccde.gif"></mapping></pre>
pend	<pre></pre>
	<pre>dmapping key="assx" value="icasx.gif" Editrext="microsoft sharePoint Designer"</pre>
pend	Control="SharePoint.OpenDocuments"/>
	<mapping key="asmx" opencontrol="" value="icasmx.gif"></mapping>
	<mapping _opencontrol="" _value="ichtm.gif" key="asp"></mapping>
	<mapping <="" edittext="Microsoft SharePoint Designer" keý="aspx" td="" value="ichtm.gif"></mapping>

c. Click Save on the File menu, and then quit Notepad.

- 3. Delete the following registry for Microsoft PDF Protector in SharePoint 2013
 - a) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/15.0/IrmProtectors

"{FC93F6CC-D367-4FC9-B3F6-E0933A24A8C8}"

"Microsoft.Office.Irm.PdfIrmProtector"

b) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\15.0\IrmProtectors\PdfIrmProtector

"Extensions"="PDF"

"Product"="PdfIrmProtector"

"Version"="15"

- 4. Add the following registry for Foxit PDF Secure PDF Protector in SharePoint 2013
 - a) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/15.0/IrmProtectors

"{2B86FB4A-D503-4040-8843-A2195C1E1D7E}" = "PDFProtector"

b) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/15.0/IrmProtectors/PDFProtector

"Extensions"="pdf"

"Product"=" PDFProtector"

"Version"="2"

=

• For MOSS 2016

- Copy the downloaded .png file to "Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\Template\Images"
- 2. Edit the file "Drive:\Program Files\Common Files\Microsoft Shared\Web server extensions\16\Template\Xml\DOCICON.XML":
 - a. Right-click DOCICON.XML file > click Open With > select Notepad.

b. Add an entry for the .pdf extension as the file's name. For example, type the ICPDF as the name of the .png file:

<Mapping Key="pdf" Value="pdf-icon.png"/>

📕 DOCICON.XML - Notepad	
File Edit Format View Help	
OpenControl="SharePoint.OpenDocuments"/> <mapping <="" edittext="Microsoft Excel" key="ODC.Table" td="" value="icodct.gif"><td></td></mapping>	
OpenControl="ShărePoint.OpenDocuments"/> <mapping <br="" edittext="Microsoft OneNote" key="Onenote.Notebook" value="icnotebk.png">OpenControl="SharePoint.OpenDocuments"/></mapping>	
<pre>cMapping Key="PowerPoint.Slide" Value="ichtmppt.gif" EditText="Microsoft PowerPoint" (openControl="SharePoint.OpenDocuments"/></pre>	
<pre><mapping edittext="Microsoft Publisher" key="Publisher.Document" opencontrol="SharePoint.OpenDocuments" value="ichtmpub.gif"></mapping></pre>	
<pre><mapping key="SharePoint.DocumentSet" value="icdocset.gif"></mapping></pre>	it
<pre>cMapping Key="visio.WebDrawing" Value="icvdw.gif" EditText="Microsoft Visio" lopenControl="SharePoint.OpenDocuments"/></pre>	
<pre><mapping edittext="Microsoft Word" key="Word.Document" opencontrol="SharePoint.OpenDocuments" value="ichtmdoc.gif"></mapping></pre>	
<pre><mapping edittext="Microsoft InfoPath" key="XDocs.Document" opencontrol="SharePoint.OpenXMLDocuments" value="icxddoc.gif"></mapping> </pre>	
<pre><mapping key="SharePoint.Link" value="DOCLINK.GIF"></mapping></pre>	
SEVEXtension>	
<pre></pre>	
OpenControl="ShārePoint.OpenDocuments"/> <mapping key="accdt" value="icaccdb.gif"></mapping> <mapping key="accdc" value="icaccdb.gif"></mapping>	
<pre><mapping edittext="Microsoft Access" key="accde" opencontrol="SharePoint.OpenDocuments" value="icaccde.gif"></mapping></pre>	
<pre><mapping edittext="Microsoft Access" key="accdr" opencontrol="SharePoint.OpenDocuments" value="icaccde.gif"></mapping> Charping Key="accdr" Value="icaccde.gif" OpenControl="%"()</pre>	
<pre><mapping key="asax" opencontrol="" value="icasax.gif"></mapping></pre>	
<pre><mapping key="asmx" opencontrol="" value="icasmx.gif"></mapping> <mapping key="asp" opencontrol="" value="ichtm.gif"></mapping> <mapping <="" edittext="Microsoft SharePoint Designer" key="aspx" pre="" value="ichtm.gif"></mapping></pre>	
<pre><mapping <="" edittext="Microsoft SharePoint Designer" key="aspx" pre="" value="ichtm.git"></mapping></pre>	-

c. Click Save on the File menu, and then quit Notepad.

- 3. Delete the following registry for Microsoft PDF Protector in SharePoint 2016
 - a) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/16.0/IrmProtectors

"{FC93F6CC-D367-4FC9-B3F6-E0933A24A8C8}" =
"Microsoft.Office.Irm.PdfIrmProtector"

b) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\16.0\IrmProtectors\PdfIrmProtector

"Extensions"="PDF"

"Product"="PdflrmProtector"

"Version"="16"

- 4. Add the following registry for Foxit PDF Secure PDF Protector in SharePoint 2016
 - c) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/16.0/IrmProtectors

"{2B86FB4A-D503-4040-8843-A2195C1E1D7E}" = "PDFProtector"

d) HKEY_LOCAL_MACHINE/Software/Microsoft/Shared Tools/Web Server Extensions/16.0/IrmProtectors/PDFProtector

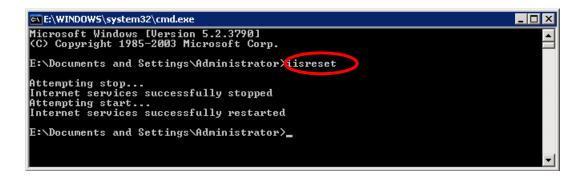
"Extensions"="pdf"

"Product"=" PDFProtector"

"Version"="2"

Perform an iisreset

1. Click Start > Run > type "cmd" in the Open dialog box> click OK > type "iisreset" at the command prompt > Enter.



2. Close the windows.

Uninstalling Foxit PDF Secure RMS Protector

To uninstall, please select one of the followings:

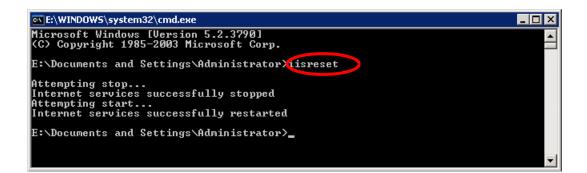
- Open the Start Menu > Settings > select "Control Panel" > click the "Add or Remove Programs" tab > click the "Foxit PDF Secure RMS Protector" record and then click the "Remove/Uninstalled" button to uninstall it.
- Open the Start Menu > Programs > select "Foxit PDF Secure RMS Protector" > click Uninstall.

Or you can double-click the SharePointPDFProtector.msi setup file that you have used to install Foxit PDF Secure RMS Protector, and perform the following:

 In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector

Selec	ct the operation you wish to perform.
Ĩ	Change
L.	Foxit PDF Secure RMS Protector has no independently selectable features.
[Repair
	Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.
[Remove
	Removes Foxit PDF Secure RMS Protector from your computer.

- Click Finish button to complete removal.
- Click Start > Run > type "cmd" in the Open dialog box> click OK > type "iisreset" in the command prompt > Press Enter.



• Close the windows.

View and Manage Event Logs of Foxit PDF Secure RMS Protector

To view and save the log information of the Protector, please do the following steps:

1. Add a registry entry.

With Administrator's Right:

HKEY_LOCAL_MACHINE/Software/Foxit Software/FXRMS/FXSPProtector

Name: trace

Type: REG_DWORD

Data: 1

Without Administrator's Right:

HKEY_CURRENT_USER/Software/Foxit Software/FXRMS/FXSPProtector

Name: trace

Type: REG_DWORD

Data: 1

Note: if the value of trace is 1, the log feature will be activated; if the value of trace is 0, the log feature will be disabled.

2. Download the **DebugView** tool from the following link and run it.

http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx

Open the tool and disable Capture Kernel feature from the "Capture" menu to avoid capturing unnecessary information.

🂐 Debug	/iew on \\SPS2003 (local)	
<u>Eile E</u> dit	Capture Options Computer	Help
🖻 🖬	✓ Capture <u>W</u> in32 Ctrl+W	🖾 🖾 () 🛆 📅 🙀
#	Capture <u>K</u> ernel Ctrl+K	g Print
	✓ Pass-Through	
	✓ <u>Capture Events</u> Ctrl+E	
	Log <u>B</u> oot	

3. Perform an iisreset command (Please refer to <u>Perform an iisreset</u>), and you will be able to see the related log information now. The log information can be saved as a .txt file.

File E	dit <u>⊂</u> apture <u>O</u> j	otions Co <u>m</u>	aputer <u>H</u> elp	
<u>N</u> ew	Window		A E> E+ ③ ⇒ ₽ A4	
Оре	n	Ctrl+O	ebug Print	-
Save	9	Ctrl+S	721 FoxitRMS: GetProductName: After URLEncodeAll	
Save	e <u>A</u> s		72]	
Log	to File	Ctrl+G	72] %0B%34%9A%5C%5C%93%9F%C6%8B%13%82%10%99%AB%94%	:59°
-	to File As	Carro	72]	
			72] FoxitRMS: FXCheckLicense: The path of the key	fi:
Print		Ctrl+P	72]	
Print	: <u>R</u> ange		72] FoxitRMS: FXCheckLicense: Foxit_CheckLicenseFi	.le
Proc	ess Crash Dump		72]	
			- 72] FoxitRMS: FXCheckLicence: the key file version	n is
Exit			72]	
43	3:38:54		[572] FoxitRMS: FXCheckLicense: It is license versio	n!
44	3:38:54	-	[572]	
45	3:38:54		[572] FoxitRMS: CProtector::HrInit success	
46	3:38:54	-	[572]	
47	3:38:54	-	[572] CReader_Register: GetHKEY: hkey = HKEY_LOCAL_M	IACI
48	3:38:54		[572]	
49	3:38:54		[572] CReader_Register::RegGetDword RegOpenKeyEx suc	cee
50	3:38:54		[572] [573] Chartenne Walarit The superson works are bus a	
51 52	3:38:54	-	[572] CProtector::HrInit The protector mode value =	1
1	3:38:54	Pn [[572]	Þ

4. If you want to disable the log feature, please set the value of trace to 0 and perform an iisreset.

Check the version of Foxit PDF Secure RMS Protector

• Please navigate to the folder where Foxit PDF Secure RMS Protector installed. Right-click PDFProtector.dll > choose Properties > click the Details tab, then you can examine the version information of Foxit PDF Secure RMS Protector:

2	PDFProtector_x6	4.dll Properties	×						
G	General Digital Signatures Security Details Previous Versions								
	Property	Value							
	Type File version Product name Product version Copyright Size Date modified Language								
	Remove Properties	and Personal Information							
		OK Cancel	Apply						

Editing Wrapper Content

If you open a PDF which is encrypted by Foxit RMS Protector with other PDF programs, a wrapper (which is actually a PDF page) will prompt you to download Foxit PhantomPDF/Reader to open the PDF. If you want to edit the wrapper content, please save the updated content as a PDF file named as "wrapperPDF" and place it within the RMS Protector's installation directory.

Configuring AD RMS to Work with SPS-SRV

Note: If you have configured AD·RMS when you were installing SharePoint, please skip this chapter.

For MOSS 2007

To add SPS-SRV to Local Intranet

1. Log on SPS-SRV as domain administrator, e.g., WIONS\administrator.

- 2. Click Start. Point to Control Panel, and then click Internet Options.
- 3. Click the **Security** tab, and choose **Local Intranet**, and then click the **Sites** button
- 4. Type **http://SPS-SRV**, and then click **Add**. Note: SPS-SRV is the computer's name of MOSS server.
- 5. Click Close, and then choose OK

To add SPS-SRV to the AD·RMS Certification Pipeline

- 1. Log on ADRMS-SRV as CPANDL\Administrator.
- 2. Click **Start**, and then click **Computer**.
- 3. Navigate to C:\Inetpub\wwwroot_wmcs\Certification.
- 4. Right-click **ServerCertification.asmx**, and choose **Properties**, and then click the **Security** tab.
- 5. Click Advanced>Edit, and select the check box Include inheritable permissions from this object's parent. Then click OK two times.
- 6. Click **Edit**, and then click **Add**.
- 7. Click **Object Types**, and select the check box **Computers**, then click **OK**.
- 8. Type the computer's name of MOSS server, such as **SPS-SRV**, and then click **OK**.
- Click OK to close the ServerCertification.asmx Properties sheet.
 The default Read & Execute and Read permissions are configured for the SPS-SRV computer account object and other accounts' are all inherited from the parent folder.
- 10. Click **Start**, and then click **Command Prompt**.
- 11. Type **iisreset**, and then press ENTER.

To activate Information Rights Management in Office SharePoint Server 2007

Please do the following:

- 1. Log on SharePoint Server as the administrator.
- 2. Click **Start**, and point to **Administrative Tools**, then click **SharePoint 3.0 Central Administration**.
- 3. Click **Operations**, and choose **Information Rights Management**.
- 4. Click Use the default RMS server specified in Active Directory.
- 5. Click OK.

To restrict permissions using AD·RMS

1. Log on as CPANDL\administrator.

- 2. Click Start, point to All Programs, and then click Internet Explorer.
- 3. Type http://SPS-SRV in the address bar, and then click Go.
- 4. Click **Shared Documents**, and choose **Library page**, and then click **Library Settings button**.
- 5. Under the **Permissions and Management** heading, click **Information Rights Management.**
- 6. Select the check box **Restrict permission to documents in this library on download.**
- 7. Type **CPANDL Protected** in the **Permissions policy title** box.
- 8. Type **Restrict CPANDL employees from printing** in the **Permission policy description** box.
- 9. Click OK.

For MOSS 2010

To add SPS-SRV to Local Intranet

- Log on SPS-SRV as domain administrator, e.g., CPANDL\administrator.
- Click **Start**, and point to **Control Panel**, then choose **Internet Options**.
- Click the **Security** tab, and choose **Local Intranet**, and then click the **Sites** button.
- Type http://SPS-SRV, and then click Add. Note: SPS-SRV is the computer's name of MOSS2010 server.
- Click Close, and then click OK.

To add SPS-SRV to the AD·RMS Certification Pipeline

- Log on ADRMS-SRV as CPANDL\Administrator.
- Click **Start**, and then click **Computer**.
- Navigate to C:\Inetpub\wwwroot_wmcs\Certification.
- Right-click **ServerCertification.asmx**, and click **Properties**, then choose the **Security** tab.
- Click **Advanced** and choose the **Edit**. Select the check box **Include inheritable permissions from this object's parent**, and then click **OK** two times.
- Click **Edit**, and then click **Add**
- Click **Object Types**, select the check box **Computers**, and then click **OK**
- Type the computer's name of MOSS server, such as **SPS-SRV**, and then click **OK**
- Click **OK** to close the **ServerCertification.asmx Properties** sheet. The default Read & Execute and Read permissions are configured for the SPS-SRV computer account object and other accounts are all inherited from the parent folder.

- Click **Start**, and then click **Command Prompt**.
- Type iisreset, and then press ENTER

To activate Information Rights Management in Office SharePoint Server 2010

Please do the followings:

- Log on SharePoint Server as administrator.
- Click **Start**, and point to **Administrative Tools**, then click **SharePoint 2010 Central Administration**.
- Click Security (on the left), and then click Configure Information Rights Management under the Information policy heading.
- Click Use the default RMS server specified in Active Directory.
- Click **OK**.

To restrict permissions using AD·RMS

- Log on as CPANDL\administrator.
- Click **Start**, point to **All Programs**, and then click **Internet Explorer**.
- Type **http://SPS-SRV** in the address bar, and then click **Go**.
- Click **Shared Documents**, and choose **Library page**, and then click **Library Settings button**.
- Under the **Permissions and Management** heading, click **Information Rights Management**.
- Select the check box **Restrict permission to documents in this library on download**.
- Type **CPANDL Protected** in the **Permissions policy title** box.
- Type **Restrict CPANDL employees from printing** in the **Permission policy description** box.
- Click OK.

For MOSS 2013 and 2016

To add SPS-SRV to Local Intranet

- Log on SPS-SRV as domain administrator, e.g., MOSS\administrator.
- Click **Start**, and go to **Control Panel**, then choose **Internet Options**.
- Click the **Security** tab, and choose **Local Intranet**, and then click the **Sites** button.

- Type http://SPS-SRV, and then click Add. Note: SPS-SRV is the computer's name of MOSS 2013 or 2016 server.
- Click Close, and then click OK.

To add SPS-SRV to the AD·RMS Certification Pipeline

- Log on ADRMS-SRV as MOSS\Administrator.
- Click Start, and then click Computer.
- Navigate to C:\Inetpub\wwwroot_wmcs\Certification.
- Right-click **ServerCertification.asmx**, and click **Properties**, then choose the **Security** tab.
- Click **Advanced** and choose the **Edit**. Select the check box **Include inheritable permissions from this object's parent**, and then click **OK** two times.
- Click **Edit**, and then click **Add**
- Click **Object Types**, select the check box **Computers**, and then click **OK**
- Type the computer's name of MOSS server, such as **SPS-SRV**, and then click **OK**
- Click **OK** to close the **ServerCertification.asmx Properties** sheet. The default Read & Execute and Read permissions are configured for the SPS-SRV computer account object and other accounts are all inherited from the parent folder.
- Click **Start**, and then click **Command Prompt**.
- Type **iisreset**, and then press ENTER

To activate Information Rights Management in Office SharePoint Server 2013 and 2016

Please do the followings:

- Log on SharePoint Server as administrator.
- Click Start, and point to Administrative Tools, then click SharePoint 2013 (or 2016) Central Administration.
- Click Security (on the left), and then click Configure Information Rights Management under the Information policy heading.
- Click Use the default RMS server specified in Active Directory.
- Click **OK**.

To restrict permissions using AD·RMS

- Log on as MOSS\administrator.
- Click Start, go to All Programs, and then click Internet Explorer.

- Type http://SPS-SRV in the address bar, and then click Go.
- Click **Documents**, and choose **Library page**, and then click **Library Settings button**.
- Under the **Permissions and Management** heading, click **Information Rights Management**.
- Select the check box **Restrict permission on this library on download**.
- Type **CPANDL Protected** in the **Create a permissions policy title** box.
- Type **Restrict CPANDL employees from printing** in the **Add a permission policy description** box.
- Click OK.

Working with Foxit PDF Secure RMS Protector

For MOSS 2007

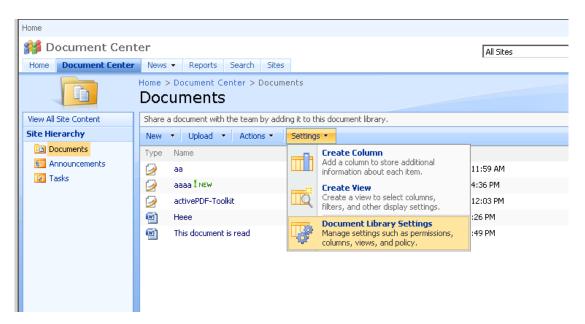
To add the domain user to SharePoint site

- In the same Office SharePoint Server 2007 site, click **Home**.
- Click Site Actions and point to Site Settings, and then click People and Groups.
- Click New, and then choose Add Users.
- Type domain users' names, such as **Ind1@cpandl.cn;Ind2@cpandl.cn** in the **Users/Groups** box, and then click **OK**. A list of users who have the permission to use the SharePoint will be displayed.

Home > Site Settings > Permissions > Add Users Add Users: Home	
Use this page to give new permissions.	
Add Users You can enter user names, group names, or e-mail addresses. Separate them with semicolons. Add all authenticated users	Users/Groups: Ind1@cpandl.cn;Ind2@cpandl.cn
Give Permission Choose the permissions you want these users to have. You can add users to a SharePoint group (which is already assigned to a permission level), or you can add users individually and assign them to a specific permission level. SharePoint groups are recommended as they allow for ease of permission management across multiple sites.	Give Permission C Add Users to a SharePoint group Home Members [Contribute] View permissions this group has on sites, lists, and items C Give users permission directly Full Control - Has full control. Design - Can view, add, update, delete, approve, and customize. Manage Hierarchy - Can create sites and edit pages, list items, and documents. Approve - Can view, add, update, and delete. Read - Can view nady. Read: - Can view pages and documents, but cannot view historical versions or review user rights information. Weiw Only - Members of this group can view pages, list items, and documents. Weiw Only - Members of this group can view pages, list items, and documents. Weiw Only - Members of this group can view pages, list items, and documents, the document has a server-side file handler.

To set the group permission in SharePoint site

• Navigate to the **Documents** page, log on as administrator@cpandl.com, clicking the **Settings** drop-down box and select **Document Library Settings**.



- Click **Permissions for this document library** under Permissions and Management on the Customize Documents page.
- Please click **Home Members** on "Permissions: Documents" page.
- Please choose the permission you need, for example, you can choose the **Contribute-Can view, add, update, and delete**. Then click **OK**.

ome		Welcome administrator ▼ My Site My Links ▼
🕌 Document Ce	enter	
Home Document Cen	nter News - Reports Search Sites	Site Action
	Home > Document Center > Documents > Settings > Permissions > Edit Permissions Edit Permissions: Documents	
	Users or Groups The permissions of these users or groups will be modified.	Users: Home Members
	Choose Permissions Choose the permissions you want these users or groups to have.	Permissions: Full Control - Has full control. Design - Can view, add, update, delete, approve, and customize. Manage Herarchy - Can create sites and edit pages, list items, and documents. Approve - Can edit and approve pages, list items, and documents. Contribute - Can view, add, update, and delete. Read - Can view only. Restricted Read - Can view pages and documents, but cannot view historical versions or review user rights information. View Only Nembers of this group can view pages, list items, and accuments. If the document has a server-side file handler available, they can only view the document using the server-side file handler.

• Return to **Documents** page, log on as Ind1@cpandl.com, to download a PDF file to your host.

Document Ce	ter News - Reports Search Sites	All Sites	Advanced Search
	Home > Document Center > Documents Documents		
iew All Site Content	Share a document with the team by adding it to this document library.		
ite Hierarchy	New - Upload - Actions -		View: All Documents
Documents	Type Name	Modified	Modified By
Announcements	000120_CHS_500/F	5/8/2011 8:19 PM	administrator
Tasks	2000228 CHS 200000	▼ 5/19/2011 3:02 AM	Ind 1
	000436_CHS_As Open in New Tab	5/8/2011 8:20 PM	administrator
	1 Open in New Window	5/8/2011 8:10 PM	administrator
	10paatopp Save Target As	5/8/2011 8:10 PM	administrator
	2 Print Target	5/8/2011 8:10 PM	administrator
	aaaa Cut Copy	4/2/2009 12:49 AM	Ind 1
	Copy of 2008-0 Copy Shortcut 408	5/8/2011 8:10 PM	administrator
	doc3 Paste	5/8/2011 8:10 PM	administrator
	double letters Add to Favorites	4/2/2009 12:39 AM	administrator
	Properties	5/8/2011 8:12 PM	administrator
	FoxitPDFIFilter1:urorsQcserver2005_manuar	5/8/2011 8:17 PM	administrator
	FoxitPDFIFilter 1.0 for WDS and Vista Search_Manual	5/8/2011 8:12 PM	administrator
	FoxitPDFIFilter 1.0for/WSS_manual	5/8/2011 8:18 PM	administrator
	2 n1256	5/8/2011 8:11 PM	administrator
	news2	5/8/2011 8:11 PM	administrator
	en test	4/2/2009 12:26 AM	administrator
Recycle Bin	VacuInstalmanual	5/8/2011 8:11 PM	administrator

• Open the download PDF file by Foxit Reader, and left-click **View Permission** to see the **RMS Right**.

FoxitPhantomPDF51_Qu	ocument Properties Description Security Fonts		
WINOS Protected - Res	Document Security Security Method: RMS Encry	ption	view permission ×
	Protection Policy Information		
	WINOS Protected - Restrict WINOS er	nployees from printing	
	The following users have permission to a	access this document:	
	User	RMS Right	
	emily1@winos.cn	Change	
P	PDF Rights		
0	VIEW: Allowed OWNER: Not Allowe	ed	
	VIEW RIGHTS DATA: Not Allow PRINT: Not Allow	ed	
	PRINT HIGH: Not Allow FILL FORM: Allowed ANNOTATE: Allowed	ea	
	ASSEMBLE: Allowed MODIFY: Allowed		
	EXTRACT ACCESS: Allowed EXTRACT: Allowed		
E	License Expiration date: Unlimited	Content Expiration date: 2012-04-07T07:29	
L.		OK Cancel	

To restrict the print permissions using RMS

- In the same Office SharePoint Server 2007 site, click Home.
- Click **Document Center**, and then click **Documents**.
- On the **Documents** page, left-clicking the **Settings** drop-down box and select **Document Library Settings**.
- On settings page, choose **Information Rights Management** under Permissions and Management.
- Choose Allow users to print documents, and then click OK.

Home		Welcome administrator 🔻 My Site My Links 🔻 🧯
🎁 Document Ce	enter	
Home Document Cen	ter News - Reports Search Sites	Site Actions 🔻
	Home > Document Center > Documents > Settings > Information Rights Management Information Rights Management Settings	t Settings
	Information Rights Management (IRM) IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this server.	 Restrict permission to documents in this library on download: Permission policy title: CPANDL Protected Example: Company Confidential Permission policy description: Restrict WINOS employees from printing
		OK Cancel

• Return to **Documents** page, for example log on as Ind1@cpandl.cn, right-click a pdf file and **choose Save Target AS...** to save a PDF file to the local host.

Document Ce	ter News • Reports Search Sites	All Sites	Advanced Search
	Home > Document Center > Documents Documents		
ew All Site Content	Share a document with the team by adding it to this document library.		
te Hierarchy	New - Upload - Actions -		View: All Documents
Documents	Type Name	Modified	O Modified By
Announcements	000120_CHS_500/f	5/8/2011 8:19 PM	administrator
Tasks	000228 CHS 20 Open	5/19/2011 3:02 AM	Ind 1
	000436_CHS_As Open in New Tab	5/8/2011 8:20 PM	administrator
	1 Open in New Window	5/8/2011 8:10 PM	administrator
	10paatopp Save Target As Print Target	5/8/2011 8:10 PM	administrator
	2	5/8/2011 8:10 PM	administrator
	aaaa Cut Copy	4/2/2009 12:49 AM	Ind 1
	Copy of 2008-0 Copy Shortcut 408	5/8/2011 8:10 PM	administrator
	🖉 doc3 Paste	5/8/2011 8:10 PM	administrator
	double letters Add to Favorites	4/2/2009 12:39 AM	administrator
	FoxitPDFIFiter 1 Properties	5/8/2011 8:12 PM	administrator
	FoxitPDFIFilter1:urorsQcserver2005_manual	5/8/2011 8:17 PM	administrator
	FoxitPDFIFilter1.0forWDSandVistaSearch_Manual	5/8/2011 8:12 PM	administrator
	FoxitPDFIFilter1.0forWSS_manual	5/8/2011 8:18 PM	administrator
	n1256	5/8/2011 8:11 PM	administrator
	news2	5/8/2011 8:11 PM	administrator
	en test	4/2/2009 12:26 AM	administrator
Recycle Bin	VacuInstalmanual	5/8/2011 8:11 PM	administrator

• Open the download PDF file by Foxit Reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following picture.

FoxitPhantomPDF51_Qu	ocument Properties		
File Edit View Tools	Description Security Fonts		
WINOS Protected - Res	Document Security		🖉 view permission 🛛 ×
WINOS Protected - Res	Security Method: RMS Encryption		view permission
	Protection Policy Information		
	WINOS Protected - Restrict WINOS employ	ees from printing	
	The following users have permission to acces	s this document:	
	User	RMS Right	
	emily1@winos.cn	Change	
🗣	PDF Rights		
A	VIEW: Allowed		
0	OWNER: Not Allowed VIEW RIGHTS DATA: Not Allowed		
2	PRINT: Allowed		
	PRINT HIGH: Allowed		
	FILL FORM: Allowed ANNOTATE: Allowed		
	ANNOTATE: Allowed ASSEMBLE: Allowed		
	MODIFY: Allowed		
	EXTRACT ACCESS: Allowed		
	EXTRACT: Allowed		
	License Expiration date: Unlimited	Content Expiration date: Unlimited	
F		OK Cancel	

For MOSS 2010

To add the domain user to SharePoint site

- Click Start, and point to All Programs, then click Internet Explorer.
- Type http://SPS-SRV in the address bar, and then click **Go**. This operation will open the default Office SharePoint Server 2010 site that was created during installation.
- Click Site Actions, and point to Site Settings, and then click People and Groups under the Users and Permissions heading.
- Click **New**, and then click **Add Users**.
- Type domain users' names, such as **Ind1@cpandl.cn;Ind2@cpandl.cn** in the **Users/Groups** box, and then click **OK**. A list of users who have the permissions to use the SharePoint will be displayed.

Grant Permissions		
Select Users You can enter user names, group names, or e-mail addresses. Separate them with semicolons.	Users/Groups: Ind1@cpandl.com	s. 19
	ОК	Cancel

To set group permission in SharePoint site

Log on as CPANDL\Administrator.

Click Start, and point to All Programs, and then click Internet Explorer.

Type http://SPS-SRV in the address bar, and then click Go.

Click Shared Documents and Library page, then click Library Settings button.

Site Actions 👻 🐋	2	Browse Page)				
Edit Check Out	Edit Properti	Rename	Page History Page Permissions	E-mail a Link	Make Incoming Homepage	Library Settings Library Permissions	View All Pages
Edit		Manag	e	Share & Track	Page Actions	Page Library	
Libraries Site Pages Shared Documents	9	Welcon	ne to your	site!			
Lists					r add new lists to this s or on the calendar		
Calendar		You can click on Shared Documents to add files or on the calendar to create new team events. Use the links in the getting started section to share your site and customize its look.					
Tasks							
		Shared Do	cuments				
Discussions Team Discussion		🗌 Туре	Name		I	Modified	Modified By
		2	000120_CH clea	in2 no print	5	5/12/2011 2:16 PM	System Account
🗟 Recycle Bin			000120_CH Ind1	l spsvc		5/14/2011 3:45 PM	System Account
					5	0/14/2011 3:45 PM	System Account
	t	2	000120_CH Ind1	L		5/14/2011 3:40 PM	Ind1
All Site Content	t	-	000120_CH Ind1 000120_CH	L	5		
	t	2	-		1	5/14/2011 3:40 PM	Ind1

• Click **Permissions for this document library** under Permissions and Management on Customize Documents page.

	s10-sps64/_layouts/user.aspx?obj=%7BAA3E30E8%2D10E5%2D40FE	100000 12 /020/ME 10 100000 /070,000000	
Favorites 🛛 🚖 🌄 Sug	gested Sites 👻 🙋 Web Slice Gallery 👻		
Permissions: Site Pages			
	Permission Tools		
ite Actions 👻 対 Brow	/se Edit		
🚱 🍃	A		
Anage Stop Inheriting Parent Permissions F	Check Permissions		
Inheritance	Check		
Libraries	edit files uploaded to wiki pages are controlled by the librar Name	Туре	Permission Levels
	adrms test Members	SharePoint Group	
Site Pages Shared Documents			Contribute
			Full Control
Shared Documents	adrms test Owners	SharePoint Group	Tall Collaron
	adrms test Uniters	SharePoint Group	
ists	adrms test Visitors	SharePoint Group	Read
lists Calendar	adrms test Visitors System Account (SHAREPOINT\system)	SharePoint Group User	Read Limited Access
lists Calendar Tasks	adrms test Visitors	SharePoint Group	Read Limited Access
Lists Calendar Fasks	adrms test Visitors System Account (SHAREPOINT\system)	SharePoint Group User	Read Limited Access
Lists Calendar Fasks Discussions	adrms test Visitors System Account (SHAREPOINT\system)	SharePoint Group User	Read Limited Access
Lists Calendar Tasks Discussions Team Discussion	adrms test Visitors System Account (SHAREPOINT\system)	SharePoint Group User	Read Limited Access

• Return to **Shared Documents** page, log on as Ind1@cpandl.com(one of ADRMS test Members), to download a PDF file to your load host.

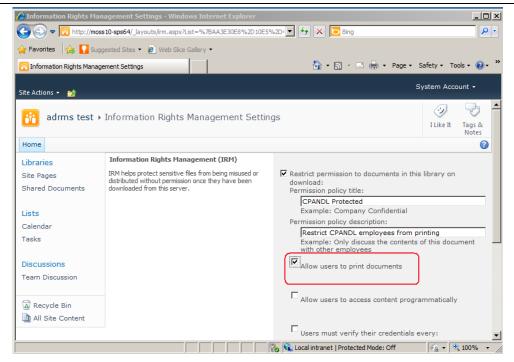
Home > Sha		nts Library ents ► All Documents ~ m by adding it to this documen	t library.		
Home				Search this site	۵ م
Libraries Site Pages Shared Documents Lists	Type	Name 0000582_text field II NEW 2 big and small-admin II NEW		Modified 4/6/2012 9:39 AM 3/22/2012 4:42 PM 4/6/2012 2:20 PM	Modified By administrator administrator Ind1 Ind1
Calendar Tasks Discussions Team Discussion		Foxit Sharepoint PDF Protec FoxitPhantomPDF51_QuickG metadata INEW pdf_reference1.7 INEW 月项目进度汇报		3/5/2012 8:20 PM - 4/6/20 12 9:39 AM 12 9:38 AM 12 9:39 AM 12 7:17 PM	administrator administrator administrator administrator
All Site Content	🖶 Add docu	iment	Cut Copy Copy Shortcut Paste		

• Open the download PDF file by Foxit Reader, and left-click **View Permission** to see the **RMS Right**.

FoxitPhantomPDF51_Qu	cument Properties	onts				
WINOS Protected - Res	Document Security Security Method:	RMS Encryption				view permission ×
	WINOS Protected - Restrict					
	The following users have perm	nission to access				
	User		RMS Right			
	emily1@winos.cn		Change			
P	PDF Rights					
0	VIEW: OWNER:	Allowed Not Allowed				
	VIEW RIGHTS DATA: PRINT:	Not Allowed Not Allowed				
-	PRINT HIGH:					
	FILL FORM:	Allowed				
	ANNOTATE:	Allowed				
	ASSEMBLE:	Allowed				
	MODIFY:					
	EXTRACT ACCESS:	Allowed				
	EXTRACT:	Allowed				
E	License Expiration date: Unlin	nited	Content Expiratio	n date: 2012-04-07T07:	29	
				ОК	Cancel	Ţ

To restrict the print permissions using RMS

- In the same Office SharePoint Server 2010 site, click Home.
- Click Shared Documents and Library page, then click Library Settings button.
- On the settings page, choose **Information Rights Management** under Permissions and Management.
- Choose Allow users to print documents, and click OK.



• Return to **Shared Documents** page, for example log on as Ind1@cpandl.com, and right-click a pdf file and **choose Save Target AS...** to save a PDF file to the local host.

Bhare a docum		ents All Documents m by adding it to this document	t library.		
Home				Search this site	۵ م
Libraries	🗌 Туре	Name		Modified	Modified By
Site Pages	Ø	0000582_text field 🗱 NEW		4/6/2012 9:39 AM	administrator
Shared Documents		2		3/22/2012 4:42 PM	administrator
		big and small-admin 🛢 NEW		4/6/2012 2:20 PM	Ind1
Lists Calendar	1	Foxit Sharepoint PDF Protec	tor user manual2	3/5/2012 8:20 PM	Ind1
Calendar Tasks		FoxitPhantomPDF51 QuickG			administrator
Tasks	2	metadata 🗮 NEW	Open Open in New Tab	12 9:38 AM	administrator
Discussions		pdf_reference1.7 🗮 NEW	Open in New Window	12 9:39 AM	administrator
Team Discussion		月项目进度汇报	Save Target As	12 7:17 PM	administrator
	🕈 Add doci	iment	Print Target		
Recycle Bin	- //00 0000		Cut		
All Site Content			Copy Copy Shortcut		

• Open the download PDF file by Foxit Reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following picture.

FoxitPhantomPDF51_Qu	Document Properties Description Security Fonts		
WINOS Protected - Res	Document Security Security Method: RMS Encrypti	on	view permission ×
	Protection Policy Information		
	WINOS Protected - Restrict WINOS employed	oyees from printing	
	The following users have permission to acc	ess this document:	
7	User	RMS Right	
	emily1@winos.cn	Change	
P	PDF Rights		
0	VIEW: Allowed OWNER: Not Allowed		
	VIEW RIGHTS DATA: Not Allowed PRINT: Allowed PRINT HIGH: Allowed		-
	FILL FORM: Allowed ANNOTATE: Allowed		
	ANNOTATE: Allowed ASSEMBLE: Allowed		
	MODIFY: Allowed		
	EXTRACT ACCESS: Allowed		
	EXTRACT: Allowed		
	License Expiration date: Unlimited	Content Expiration date: Unlimited	
		OK Cancel	

For MOSS 2013 and 2016

To add the domain user to SharePoint site

- Click Start, and go to All Programs, then click Internet Explorer.
- Type http://SPS-SRV in the address bar, and then click **Go**. This operation will open the default Office SharePoint Server 2013 (or 2016) site that was created during installation.
- Click Setting, and go to Site Settings, and then click People and Groups under the Users and Permissions heading.
- Click New, and then click Add Users.
- Type domain users' names, such as **rms01@moss.com;rms02@moss** in the **Users/Groups** box, and then click **OK**. A list of users who have the permissions to use the SharePoint will be displayed.

Share 'Home'		
Add people to the Home Members group		
rms01 x rms02 x		
	Share	Cancel

To set group permission in SharePoint site

Log on as MOSS\Administrator.

Click **Start**, and go to **All Programs**, and then click **Internet Explorer**.

Type http://SPS-SRV in the address bar, and then click Go.

Click **Documents** and **Library page**, then click **Library Settings button**.

SharePoint			Newsfe	ed SkyDrive S	ites Ac	dministrator 🗸 🔅 🕇
BROWSE FILES LIBR	(ARY			Q	SHARE 🏠	FOLLOW 🔂 SYNC [
	Current View:	E-mail a Link SS Feed Most Popular Items Share & Track	Tags & Notes Tags and Notes	Connect to Outlook Connec Connect & Exp	- L	ustomize library - Settings
Home	⊕ new d	ocument or drag	g files here			
Documents	All Document	ts Approve/reject Ite	ems My subr	missions •••	Find a file	e p
Site Contents	 D 	Name		Mo	dified	Modified By
EDIT LINKS		BNET_BestPractices_M	anagingEmplo	yees 🚥 Jar	iuary 31	🗌 Administrato
		Button Menultems		••• Fel	oruary 21	🗌 Administrato
		dd		••• Fel	oruary 21	🗌 Administrato
		Foxit PDF Secure RMS	Protector Man	ual 💀 Fel	oruary 21	🗌 Administrato

• Click **Permissions for this document library** under Permissions and Management on Customize Documents page.

SharePoint		Newsfeed SkyDr	rive Sites	Administr	ator 🗸 🔅	
BROWSE PERMISSIONS				🗘 SHARE	☆ FOLLOW	
anage Stop Inheriting Permissions Inheritance Check	ons					
Home	This library inherits permission	s from its parent. (Home	e)			
Documents						
Site Contents	Name Name	Туре	Permission Lev	vels		
🖋 EDIT LINKS	Excel Services Viewers	SharePoint Group	View Only			
	Home Members	SharePoint Group	Edit, Contrib	oute		
	Home Owners	SharePoint	Full Control			
		Group				
	Home Visitors	Group SharePoint Group	Read			
		SharePoint				

• Return to **Documents** page, log on as <u>rms01@moss.com</u> (one of ADRMS test Members), to download a PDF file to your load host.

SharePoint	Newsfeed SkyDrive Sites ms01 -
BROWSE FILES LIBRARY Home	☆ FOLLOW 및 SYNC [=
Documents	All Documents My submissions ···· Find a file
Site Contents	✓ Name Modified Modified By Image: BNET_BestPractices_ManagingEmployees January 31 □ Administrato
	Image: Button MenuItems February 18DefinitionImage: Button MenuItems
	Foxit PDF Secure RMS Protector Manual January 30 Administrato Open
	図 SubmitForm Open in new tab Administrato ● word Save target as Administrato ● 加班管理办法-20120917_decrypted Print target Administrato

• Open the download PDF file by Foxit Enterprise Reader, and left-click **View Permission** to see the **RMS Right**.

📶 🍃 🗄 🖶 🖃 約 🥎 🕫	Foxit_PDF_Secure_RMS	_Protector_Manual.pdf (SECURED) - Foxit Reader	
FILE HOME REVIEW	Document Properties	r (* 1)	₽ ∰ • ↓ _ ▲
Hand Select Annotati Select Text Select Annotati Text Select Annotati Ty Typewriter Solet Tools	Description Security Fonts Document Security Security Method: RMS Encryption		i Link File Attachment Multimedia
MOSS restrict - MOSS restrict	Protection Policy Information MOSS restrict - MOSS restrict You are currently authenticated to view this rms01@moss.com	document as:	View Permission ×
	PDF Rights Full control: View document: Print with low resolution: Print with high resolution: Fill in a form: Comment in the document: Manage pages and bookmarks: Modify document: Content copying for accessibility: Extract the contents of the document: Run java script: License Expiration days: 30	Not Allowed Allowed Not Allowed Allowed Allowed Allowed Allowed Allowed Allowed Allowed Not Allowed Content Expiration date: Unknown	
		OK	.46% ▼ □ ⊕ //

To restrict the print permissions using RMS

- In the same Office SharePoint Server 2013 (or 2016) site, click Home.
- Click **Documents** and **Library** page, then click **Library Settings button**.
- On the settings page, choose **Information Rights Management** under Permissions and Management.
- Choose Allow viewers to print, and click OK.

SharePoint	Newsfeed SkyDrive Sites Administrator 🗸 🔅 ?
	♥ SHARE ☆ FOLLOW [□]
Site Contents	Restrict permissions on this library on download Create a permission policy title
	MOSS restrict Add a permission policy description:
	Add a permission policy description:
	HIDE OPTIONS
	Set additional IRM library settings This section provides additional settings that control the library behavior. Do not allow users to upload documents that do not support IRM Stop restricting access to the library at 4/12/2013
	Configure document access rights This section control the document access rights (for viewers) after the document is downloaded from the library right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized use Allow viewers to print Allow viewers to run script and screen reader to function on downloaded documents Allow viewers to write on a copy of the downloaded document After download, document access rights will expire after these number of days (1-365) 90
<	>

• Return to **Documents** page, for example log on as rms01@moss.com, and right-click a pdf file and **choose Save Target AS...** to save a PDF file to the local host.

SharePoint	Newsfeed SkyDrive Sites ms01 - 🔅 ?
BROWSE FILES LIBRARY Home	☆ FOLLOW 및 SYNC (☐ (+) new accument or arag tiles nere
Documents	All Documents My submissions ···· Find a file
Site Contents	✓ □ Name Modified By Image: BNET_BestPractices_ManagingEmployees January 31 □
	I Button MenuItems ···· February 18
	 ✓ 認 Foxit PDF Secure RMS Protector Manual GubmitForm Word ● 加班管理办法-20120917_decrypted ● Administrator ● Print target ● Administrator

• Open the download PDF file by Foxit Reader. Left-click **View Permission** to view the RMS Right of this file. Please see the following picture.

🏭 🍃 🗄 🖶 🖃 🐐 🥠 🔿 =	Foxit_PDF_Secure_RMS_Protector_Manual.pdf (SECURED) - Foxit Reader	
FILE HOME REVIEW	Document Properties	
Hand Select Annotation Select Typewriter Text Note Tools	Description Security Fonts Document Security Security Method: RMS Encryption	Link File Attachment Multimedia Insert View Permission ×
•	Protection Policy Information	
	MOSS restrict - MOSS restrict You are currently authenticated to view this document as:	
	rms01@moss.com	
€ 	Full control: Not Allowed	
B	View document: Allowed Print with low resolution: Allowed	
4	Print with low resolution: Allowed Print with high resolution: Allowed	
0	Fill in a form: Allowed	
	Comment in the document: Allowed	
	Manage pages and bookmarks: Allowed Modify document: Allowed	
_1	Content copying for accessibility: Allowed	
de la constante de la constant	Extract the contents of the document: Allowed	
	Run java script: Not Allowed	
	License Expiration days: 30 Content Expiration date: Unknown	1000
	OK	
		7.24% • ⊖ — • //

Client, Outlook 2010

Chapter 3 - For Exchange

Getting Started

This section provides everything about getting started with Foxit PDF Secure RMS Protector you'll need to know, including its system requirements, install and uninstall instructions.

System Requirements

Client

Computer **Operating System** Requirement ADRMS Server RMS, Internet Information Services Windows Server 2008 R2 (IIS) 6.0, World Wide Web Publishing Service, Message Queuing (also known as MSMQ) DC Windows Server 2003 Active Directory, Domain with SP1 System (DNS) ADRMS-DB Windows Server 2003 Microsoft SQL Server[™] 2005 with SP1 Exchange Server 2010 and has been Exchange Server 2010 Windows Server 2008 added this Server to DC Such as named EX01 with SP2 or Windows Server 2008 R2

System requirements for Exchange2010

System requirements for Exchange2013

Win7

Computer	Operating System	Requirement				
ADRMS Server	Windows Server 2008 R2	RMS, Internet Information Services				
		(IIS) 6.0, World Wide Web Publishing				
		Service, Message Queuing (also				
		known as MSMQ)				
DC	Windows Server 2008	Active Directory, Domain Name				
	with SP1	System (DNS)				
ADRMS-DB	Windows Server 2012	Microsoft SQL Server™ 2012				
Exchange Server 2013		Exchange Server 2013 and has been				
Such as named	Windows Server2012	added this Server to DC				
QA2012-EXC						
Client	Win7	Client , Outlook 2013				

Name

System requirements for Exchange2016

Computer	Operating System	Requirement				
ADRMS Server	Windows Server 2012	RMS, Internet Information Services				
		(IIS)				
DC	Windows Server 2012	Active Directory, Domain Name				
		System (DNS)				
ADRMS-DB	Windows Server 2012	Microsoft SQL Server™ 2012				
Exchange Server 2016		Exchange Server 2016 and has been				
Such as named	Windows Server2012	added this Server to DC				
QA2012-EXC						
Client	Win7	Client , Outlook 2016				

Corresponding permissions of Foxit Reader and Exchange

Exchange service provides there levels rights: Full control, Change, Read.

Level	Rights of Foxit Reader
Full control	View, Copy, Modify, Print, View Data, Access, Annotate, Fill Form,
	Assemble
Change	View, Copy, Modify, Access, Annotate, Fill Form, Assemble
Read	View

The user can only print the document if the document library IRM settings have been configured to allow document printing.

Installing Foxit PDF Secure RMS Protector on an Exchange Server

To install Foxit PDF Secure RMS Protector:

- Stop the IIS Admin service: Start > Settings > Control Panel > Administrator Tools > Services > IIS Admin Service > Stop. Close window.
- Run the Foxit PDF Secure RMS Protector Setup program to install the protector on the server.



• After installing

For Exchange2010

restart IIS, MSExchangeTransport, msftesql-Exchange:

1. Click Start > Run > type "cmd" in the Open line> click OK, and execute the following commands:

net stop MSExchangeTransport

net start MSExchangeTransport

net stop msftesql-Exchange

net start msftesql-Exchange

net start MSExchangeSearch

iisreset

Administrator: C:\Windows\system32\cmd.exe Microsoft Windows [Uersion 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\Administrator.CPANDL>net stop MSExchangeTransport The Microsoft Exchange Transport service is stopping. The Microsoft Exchange Transport service was stopped successfully. C:\Users\Administrator.CPANDL>net start MSExchangeTransport The Microsoft Exchange Transport service is starting.. The Microsoft Exchange Transport service was started successfully. C:\Users\Administrator.CPANDL>net stop msftesql-Exchange The Microsoft Exchange Transport service was started successfully. C:\Users\Administrator.CPANDL>net stop msftesql-Exchange The following services are dependent on the Microsoft Search (Exchange) service Stopping the Microsoft Search (Exchange) service will also stop these services. Microsoft Exchange Search Indexer Do you want to continue this operation? (Y/N) [N]: y The Microsoft Exchange Search Indexer service is stopping..... The Microsoft Exchange Search Indexer service was stopped successfully.

```
Administrator: C:\Windows\system32\cmd.exe

The Microsoft Exchange Search Indexer service was stopped successfully.

The Microsoft Search (Exchange) service is stopping.

The Microsoft Search (Exchange) service was stopped successfully.

C:\Users\Administrator.CPANDL>net start msftesql-Exchange

The Microsoft Search (Exchange) service is starting.

The Microsoft Search (Exchange) service was started successfully.

C:\Users\Administrator.CPANDL>net start MSExchangeSearch

The Microsoft Exchange Search Indexer service is starting.

The Microsoft Exchange Search Indexer service was started successfully.

C:\Users\Administrator.CPANDL>iisreset

Attempting stop...

Internet services successfully restarted

C:\Users\Administrator.CPANDL>iisreset

Attempting start...

Internet services successfully restarted

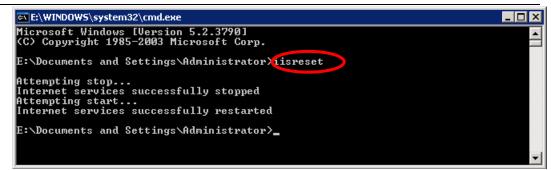
C:\Users\Administrator.CPANDL>
```

2. Close the windows.

For Exchange2013 and 2016

Restart IIS, MSExchangeTransport, MSExchangeFastSearch:

- 1. Restart MSExchangeTransport: Start > Settings > Control Panel > Administrator Tools > Services > MSExchangeTransport > Restart.
- 2. Restart MSExchangeFastSearch: Start > Settings > Control Panel > Administrator Tools > Services >MSExchangeFastSearch > Restart. Then Close the window
- 3. Restart IIS: Click Start > Run > type "cmd" in the Open dialog box> click OK > type "iisreset" at the command prompt > Press Enter.



4. Close the windows.

Uninstalling Foxit PDF Secure RMS Protector

To uninstall, please select one of the followings:

- Open the Start Menu > Control Panel->Programs->Programs and Features, and then click the "Foxit PDF Secure RMS Protector" record and then click the "Uninstall" button to uninstall it.
- Open the Start Menu > Programs > "Foxit PDF Secure RMS Protector" > Uninstall.

Or you can double-click the PDFProtector.msi setup file that you have used to install Foxit PDF Secure RMS Protector, and then do the followings:

• In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector

₩.	Foxit PDF Secure RMS Protector Setup
	Ige, repair, or remove installation ect the operation you wish to perform.
	Change Foxit PDF Secure RMS Protector has no independently selectable features.
	Repair Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.
	Remove Removes Foxit PDF Secure RMS Protector from your computer.
5	Back Next Cancel
	Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries. Remove Removes Foxit PDF Secure RMS Protector from your computer.

• Click Next button to uninstall it completely.

• For Exchange2010

Restart IIS, MSExchangeTransport, msftesql-Exchange:

1. Click Start > Run > type "cmd" in the Open line> click OK, and execute the following commands:

net stop MSExchangeTransport

net start MSExchangeTransport

net stop msftesql-Exchange

net start msftesql-Exchange

net start MSExchangeSearch

iisreset

Administrator: C:\Windows\system32\cmd.exe

 Microsoft Windows [Uersion 6.1.7600]

 Copyright (c) 2009 Microsoft Corporation. All rights reserved.

 C:\Users\Administrator.CPANDL>net stop MSExchangeTransport

 The Microsoft Exchange Transport service is stopping.

 The Microsoft Exchange Transport service was stopped successfully.

 C:\Users\Administrator.CPANDL>net start MSExchangeTransport

 The Microsoft Exchange Transport service is starting..

 The Microsoft Exchange Transport service is starting..

 The Microsoft Exchange Transport service was started successfully.

 C:\Users\Administrator.CPANDL>net stop msftesql-Exchange

 The Microsoft Exchange Transport service was started successfully.

 C:\Users\Administrator.CPANDL>net stop msftesql-Exchange

 The following services are dependent on the Microsoft Search (Exchange) service

 Stopping the Microsoft Search (Exchange) service will also stop these services.

 Microsoft Exchange Search Indexer

 Do you want to continue this operation? (Y/N) [N]: y

 The Microsoft Exchange Search Indexer service is stopping.....

 The Microsoft Exchange Search Indexer service was stopped successfully.

🕰 Administrator: C:\Windows\system32\cmd.exe	_ U ×
The Microsoft Exchange Search Indexer service was stopped successfully.	
The Microsoft Search (Exchange) service is stopping. The Microsoft Search (Exchange) service was stopped successfully.	
C:\Users\Administrator.CPANDL>net start msftesql-Exchange	
The Microsoft Search (Exchange) service is starting.	
The Microsoft Search (Exchange) service was started successfully.	
C:\Users\Administrator.CPANDL> <mark>net start MSExchangeSearch</mark>) The Microsoft Exchange Search I <mark>ndexer service is starting</mark> . The Microsoft Exchange Search Indexer service was started successfully.	
C:\Users\Administrator.CPANDLXiisreset	
Attempting stop Internet services successfully stopped Attempting start Internet services successfully restarted	
C:\Users\Administrator.CPANDL>_	-

2. Close the windows.

• For Exchange2013 and 2016

Restart IIS, MSExchangeTransport, MSExchangeFastSearch:

- 1. Restart MSExchangeTransport: Start > Settings > Control Panel > Administrator Tools > Services > MSExchangeTransport > Restart.
- 2. Restart MSExchangeFastSearch: Start > Settings > Control Panel > Administrator Tools > Services >MSExchangeFastSearch > Restart. Then Close the window
- 3. Restart IIS: Click Start > Run > type "cmd" in the Open dialog box> click OK > type "iisreset" at the command prompt > Press Enter.

📾 E:\WINDOWS\system32\cmd.exe	
Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp.	
E:\Documents and Settings\Administrator)isreset	
Attempting stop Internet services successfully stopped Attempting start Internet services successfully restarted	
E:\Documents and Settings\Administrator>_	
	•

4. Close the window.

Check the version of Foxit PDF Secure RMS Protector

• Please navigate to the folder where Foxit PDF Secure RMS Protector installed. Right-click PDFProtector.dll > choose Properties > click the Details tab, then you can examine the version information of Foxit PDF Secure RMS Protector ,as shown:

<u>a</u>)	PDFProtector_x6	4.dll Properties	x					
G	eneral Digital Sig	natures Security Details Previous Versions						
	Property	Value						
	Description -							
		Foxit PDF Secure RMS Protector X64						
	Type File version	Application extension 3.0.3.821						
	File version Product name							
	Product version							
	Copyright	Copyright © 2014 Foxit Software Inc. All						
	Size	3.19 MB						
		2014/8/22 10:50						
		Language Neutral PDFProtector.DLL						
	Onginal hiename	DIFICIECIOLDEE						
Remove Properties and Personal Information								
		OK Cancel	Apply					

Editing Wrapper Content

If you open a PDF which is encrypted by Foxit RMS Protector with other PDF programs, a wrapper (which is actually a PDF page) will prompt you to download Foxit PhantomPDF/Reader to open the PDF. If you want to edit the wrapper content, please save the updated content as a PDF file named as "wrapperPDF" and place it within the RMS Protector's installation directory.

Configuring AD·RMS to Integrate with Exchange Server in a Single Forest

Note: If you have configured AD·RMS when you were installing Exchange, please skip this operation.

To register a service connection point

- 1. Log on ADRMS server as CPANDL\ADRMSADMIN in the cluster on which you want to register an SCP.
- 2. Open the Active Directory Rights Management Services console.
- 3. Right-click the AD·RMS cluster, and then click **Properties.**
- 4. Click the **SCP** tab.
- 5. Select the **Change SCP** check box.
- 6. Click the Set the SCP to current certification cluster option, and then click OK.
- 7. Click Yes to confirm.

To give Exchange servers permissions to access the server certification

pipeline

- 1. Log on an ADRMS server as CPANDL\administrator in the AD·RMS cluster.
- 2. Click **Start**, and then click **Computer**.
- 3. Navigate to %systemdrive%\Inetpub\wwwroot_wmcs\Certification.
- 4. Right-click **ServerCertification.asmx**, and then click **Properties**.
- 5. In the **ServerCertification.asmx Properties** dialog box, click the **Security** tab.
- 6. Click the **Continue** button or the **Edit** button.
- 7. In the **Permissions for ServerCertification.asmx** dialog box, click **Add**.
- In the Select User, Computer, Service Account, or Group dialog box, click Object
 Types, and select the Computers check box, then click OK.
- 9. Type **Exchange Servers** to add the Exchange Servers group, or type the names of the Exchange servers that you want to add, separated by semicolons.
- 10. Click Check Names, and then click OK.
- 11. Under **Allow**, make sure that the **Read & execute** and the **Read** check boxes are selected.

- 12. Click **OK**.
- 13. If the AD·RMS Service Group does not appear in the **Group or user names** list, repeat the steps 6–11 to add it.
- 14. Click **OK** to close all dialog boxes.
- 15. Repeat the steps 1–14 on all other servers in the AD·RMS cluster.

To set up the Exchange Server super users group

- 1. Log on AD·RMS server as CPANDL\ADRMSADMIN, and open the Active Directory Rights Management Services console and expand the AD RMS cluster.
- 2. In the console tree, expand **Security Policies**, and then click **Super Users**.
- 3. In the Actions pane, click Enable Super Users.
- 4. In the results pane, click **Change Super User Group** to open the **Super Users** properties sheet.
- In the Super user group box, type the e-mail address of the designated super users group, or click Browse to navigate through the defined users and groups in the directory.(Such as SuperRMSAdmin@cpandl.com)
- 6. Click OK.

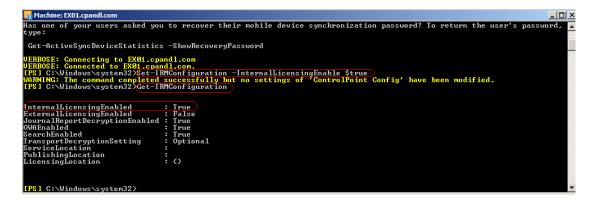
To set InternalLicensingEnable true by ExchangeManagement Shell

1. Log on as CPANDL\Administrator to Microsoft Exchange Server

- Navigate to Start->All Programs->Microsoft Exchange Server ->Exchange Management Shell
- 3. Type "Get-IRMConfiguration"

🚱 Machine: EX01.cpandl.com	
Tip of the day #47:	
You can control which features pe:	are available to Outlook Web Access users b
Set-OwaVirtualDirectory "OWA	(Default Web Site)" -ContactsEnabled \$True -
VERBOSE: Connecting to EX01.cpa VERBOSE: Connected to EX01.cpar [PS] C:\Windows\system32>Get-I]	ndl.com.
InternalLicensingEnabled	: False
ExternalLicensingEnabled	: False
JournalReportDecryptionEnabled OWAEnabled	: True : True
SearchEnabled	- True
TransportDecryptionSetting	: Optional
ServiceLocation	
PublishingLocation	:
LicensingLocation	: ()
[P8] C:\Windows\system32>_	

- 4. Type "Set-IRMConfiguration -InternalLicensingEnable \$true" to enable licensing.
- 5. Type " Get-IRMConfiguration " again ,to check InternalLicensingEnalbe is true.



Working with Foxit PDF Secure RMS Protector

For Exchange 2010

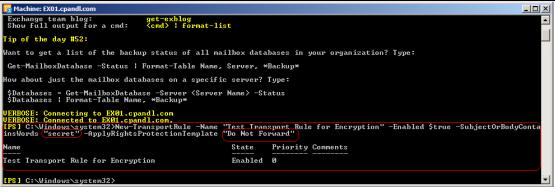
- 1. Log on as CPANDL\Administrator to EX01
- 2. Open the Exchange Management Shell.
- 3. Enter the following task and parameters:

New-TransportRule -Name "Test Transport Rule for Encryption" -Enabled \$true -

SubjectOrBodyContainsWords "secret" - ApplyRightsProtectionTemplate "Do Not Forward"

Foxit PDF Secure RMS Protector

User Manual



4. Log on as CPANDL\test to **Client,** and open **Microsoft Outlook 2010**, new an Email (for example, send an e-mail to emily1@cpandl.com). The Email includes the PDF attachment.

	9 6 🔹 🕈	· []÷	secrete test messa	ige - Message (HT	TML)		
File	Message	Insert Options	Format Text	Review			۵
	₿ JBI	Body + 11 + A* A* <u>U</u> ^a ^b ⁄⁄⁄ + <u>A</u> + Basic Text	E * E * 哟] 書 書 谆 谆 □	Address Check Book Names Names	 Attach File Attach Item * Signature * Include 	 ♥ Follow Up ▼ I High Importance Low Importance Tags T_x 	Q Zoom Zoom
	То	emily1;					
Send	Сс						
Sella	Subject:	secrete test message					
	Attached:	Microsoft SharePoin	t Server 2010.pdf (2 I	<u>(1B)</u>			
11115 15	secret test i	nessage,include the k	keyword secret.				

And then click Send.

5. Log off and log on as CPANDL\emily1 to the Client

6. Open **Microsoft Outlook 2010.** In the inbox, we can see the email which has been tested to send.

File Home Send / R	eceive Folder View		
New New E-mail Items + & Junk +	Delete Reply Reply Forward More -	Image: Second secon	ress E
New Delete	Respond	Quick Steps 🕫 Move Tags Fi	ind
Favorites Favorites Favorites Favorites Inbox Sent Items Deleted Items [1] emily1@(cpandi.com Inbox Drafts Sent Items Deleted Items [1] Outbox Sent Items Sent Sent	Search Inbox (Ctrl+E) Arrange By: Date Newest on top Today Secret test message 0 emily1 5:48 PM secret test message 0 test 5:26 PM secret two attachments 0 emily1 we only test can view, edit , 0 Administrator 3:57 PM Administrator 3:45 PM emily1 only can view test 0	Message Microsoft SharePoint Server 2010.pdf (2 MB) This is secret test message, include the keyword "secret".	ent.

7. Double click the email. We can see the email did not get forwarded. View the permission, and the detail permission is displayed as shown below-----My Permission.

M 🛛 🖓 🗘	5 🔺 🤜	- -	-		secret test mes	sage - M	essage (HTML))	_			23
File	lessage]									0	s 🕜
Delete	Reply	Reply All Resp	Forward	ų. ų -	Move to: ? To Manager Team E-mail Quick Steps	* * *	Move B +	Mark Unrea	Translat	3 -	Zoom Zoom	
to their me Conversati From:	essage an on owne test	d all rep	lies.		essage, but canno	t forward,		content. The conve	ersation own	er has fu	111 permis	
To: Cc Subject: Message This is secr		osoft Sh	arePoint S		010.pdf (2 MB) keyword "secre	You are emily 10 Do N cann owne You I View Edit: Copy Print Save Expo Acce Full c Repl Forw	e currently auth @cpandl.com ot Forward - Re ot forward, prin r has full permis have the followin : : : : : : : : : : : : :	cipients can read th t, or copy content. ssion to their messa ng permissions: programmatically:	is message, t The conversa	out ation		
 See m 	ore abou	t: test.								5	22	~

8. Double click the PDF attachment to open it. We can see the permission shown below: not allowed to be printed, copied, or accessed.

Microsoft SharePoint Server 2010 (21)	.pdf (SECURED) - Foxit Reader			
File Edit View Tools Comments	Forms Help			
	🖳 🖓 🕗 👌 📄 🔝 🦾 · 🔏	🗛 📃 📑 📓 🕞 -		
				X
U	Document Properties			view permission ×
	Description Security Fonts			·
	Document Security			
fo fo	Security Method: RMS Encry	ption	档	
	Protection Policy Information			
F	The following users have permission to a	access this document:		
0	User	RMS Right		
	emily1@cpandl.com	Change		
	test@cpandl.com	Full Control		
	PDF Rights		N+	
	VIEW: Allowed OWNER: Not Allow	ed	ΙL	
	VIEW RIGHTS DATA: Allowed			
	PRINT: Not Allow	ed		
	PRINT HIGH: Not Allow	ed		
	FILL FORM: Allowed ANNOTATE: Allowed			
	ASSEMBLE: Allowed			
	MODIFY: Allowed			
	EXTRACT ACCESS: Not Allow	ed		
	EXTRACT: Not Allow	ed		
	License Expiration date: Unlimited	Content Expiration date: Unlimited		
				-
(ОК	ancel	

For Exchange 2013 and 2016

- 1. Log on as QA2012\Administrator to QA2012-EXC
- 2. Open the Exchange Management Shell.
- 3. Enter the following task and parameters:

New-TransportRule -Name "Test Transport Rule for Encryption" -Enabled \$true -

SubjectOrBodyContainsWords "secret" - ApplyRightsProtectionTemplate "Do Not Forward"

1 2	Machine: QA2012-E)	(C.qa2012.com	x	
Welcome to the Exchange Management Shell!				
Get general help: Help Get help for a cmdlet: Help <cmdlet name=""> (Show guick reference guide: QuickRef Exchange team blog: Get-ExBlog</cmdlet>	Only Exchange cmdlets: Get-ExCommand Gmdlets that match a specific string: Help * <string>* Get general help: Help Get help for a cmdlet: Help <cmdlet name=""> or <cmdlet name=""> -? Show quick reference quide: QuickRef</cmdlet></cmdlet></string>			
Tip of the day #66:				
Do you want to remove a management role from a role group, role assignment policy, USG, or user but don't know the name of the management role assignment? Just find the role assignment with the Get-ManagementRoleAssignment cmdlet and pipe t he results to the Remove-ManagementRoleAssignment cmdlet. Type:				
Get-ManagementRoleAssignment -RoleAssignee <role assignee="" name=""> -Role <role name=""> Remove-ManagementRoleAssignment</role></role>				
UERBOSE: Connecting to QA2012-EXC.qa2012.com. UERBOSE: Connected to QA2012-EXC.qa2012.com. IPS] C:\Windows\system32>New-TransportRule -Name "Test Transport Rule for Encryption" -Enabled \$true -SubjectOrBodyConta insWords "secret" -ApplyRightsProtectionTemplate "Do Not Forward"				
Name	State Mode	Priority Comments		
Test Transport Rule for Encryption	Enabled Enforce	1		
[P8] C:\Windows\system32>_			_	

4. Log on as QA2012\Administrator to **Client**, and open **Microsoft Outlook 2013** (or **Microsoft Outlook 2016**), new an Email (for example, send an e-mail to rms1@qa2012.com). The Email includes the PDF attachment.

E .	Secrete test me	? 🗹 – 🗆 🗙				
FILE	FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW					
Paste	Calibri (Body) * 五号 * A A 二 * (二 *) 🧭	Attach Item 🗸	 Follow Up * High Importance Low Importance 			
Clipboard	Fa Basic Text F	Names Include	Tags 🕞 Zoom 🔺			
To ms1; Send						
	Subject secrete test message					
Attached 🔀 Foxit PDF Secure RMS Protector Manual.pdf (2 MB)						
This is secret test message, include the keyword "secret"						

And then click **Send.**

5. Log off and log on as QA2012\rms1 to the Client

6. Open **Microsoft Outlook 2013** (or **Microsoft Outlook 2016).** In the inbox, we can see the email which has been tested to send.

03	÷ ک 🗄			? 🗹 – 🗆 🗙
FILE	HOME SEND / RECEIVE FOLDER	VIEW		
New Email S	Items • 🖧 Junk •	€ → * ₽,	Move to:? To Manager Team Email Quick Steps To Move To Move ▼ Move Nove ■ Move Nove ■ Move ▼ Move ■ Move	Search People Control Address Book To Filter Email Find
>	Search Current Mailbox (Ctrl+E)	🔎 Current Mailbox	🔹 🗠 Reply 🕞 Reply All	
All Folders	All Unread	By Date ▼ Newest ↓	A 2013/3/14 (周四) 13:27 Administrator	
AII	Administrator secrete test message This message uses Microsoft Information	0 O 13:28	secrete test message To rms1	
L	▲ Yesterday		Permission granted by: Administrator@qa2012	2.com
	Administrator administrator trace0 This message uses Microsoft Information	0 ○ (周三) 16:28	Message 🛛 🔀 Foxit PDF Secure RMS Protect	tor Manual.pdf (3 MB)
	Administrator administratrator trace 0 test This message uses Microsoft Information	◎ ● (周三) 16:12	This is secret test message, include the keyw	ord "secret"
	Administrator administrator trace1 test This message uses Microsoft Information	َ ◎ ● (周三) 16:00	See more about Administrator.	
TEMS: 1	9 UNREAD: 4	UPDATING Inbox. CON	NECTED TO: MICROSOFT EXCHANGE 🛛 🗐 – ——	+ 100%

7. Double click the email. We can see the email did not get forwarded. View the permission, and the detail permission is displayed as shown below-----My Permission.

💌 🔒 🍤 🖑 🛧 🤟 🗧 🗧 secrete test message	- Message (HTML) ? 🗈 — 🗖 🗙
FILE MESSAGE	
Image: Delete Reply Reply Forward Image: Team Email Image: Team Email	Move Follow Up + Follow Up + Zoom
Delete Respond Quick Steps 🕞	
2013/3/14 (周四) 13:27	My Permission
Administrator	You are currently authenticated to view this message as:
secrete test message	rms1@qa2012.com
To rms1	rms1 - rms1
f) rms1 - rms1	
Permission granted by: Administrator@qa2012.com	You have the following permissions:
Message 😪 Foxit PDF Secure RMS Protector Manual.pdf (3 MB)	View: Yes Edit: No
	Copy: No
	Print: No
This is secret test message, include the keyword "secret"	Save: No
	Export: No Access the message programmatically: No
	Full control: No
	Reply: No
	Reply All: No
	Forward: No
	ОК
See more about Administrator.	

8. Double click the PDF attachment to open it. We can see the permission shown below: not allowed to be printed, copied, or accessed.

No (1)	Foxit PDF Secure RMS Protector Manual (10).pdf (SECURED) - Foxit PhantomPDF	82 - 8 X
FILE HOME EDIT ORGAN Document Pro	pperties	<u>^</u> ⊕ ▼ ⊕ ∧
Hand Select Text Select Annotation Tools Foxt PDF Secure RMS Tools Foxt PDF Secure RMS You are	Initial View Security Fonts DCR nt Security curity Method: RMS Encryption ~ Change Settings	Suspect Results V Compliance
	ights Full control: Not Allowed View document: Allowed	
	Print with low resolution: Not Allowed Print with high resolution: Not Allowed Fill in a form: Not Allowed	
0	Comment in the document: Not Allowed Manade pages and bookmarks: Not Allowed	
	Modify document: Not Allowed Content copying for accessibility: Not Allowed	
Extra	act the contents of the document: Not Allowed Run java script: Not Allowed	
License	Expiration days: Unknown Content Expiration date: Unknown OK Cancel 50.41	8% · • • · · · · · · · · · · · · · · · ·

Chapter 4 - Watermark Configuration Tool

Watermark configuration tool allows you add, edit, delete, import, and export security watermark to the files protected by RMS technology to improve the security and protect copyright of the author. This chapter will introduce the steps of using the tool.

The watermark configuration tool will pop up after finishing the installation or you can

double-click the icon losk top to open it.

4 Creating Profile

Before adding a watermark, you should create a profile first. The application will apply all of the watermarks in the profile to a PDF.

Note: you can only choose a profile but not a certain watermark to use. Please create the watermarks you want to add to one PDF in the same profile.

• Open the watermark configuration tool and check the option "Show the security watermark in protected PDF document."

□ Show the sec	Foxit PDF Secure				
Extended Settin	g				
format and can display viewer id protected files f	vtected by dynamic se only be opened by Fo lentity information on from being compromise th as screen shots, car	protected PDF ed by users cop	namic security w files. This provid ying confidentia	vatermarks a les additiona	utomatically I security to
Security Waterm	ark				Select
					8 m

- Click **Select** to open the Security Watermark Management.
- Click **New Profile** to create a profile and name it.

Security Watermark Management	×
Select profie	New Profile Add Edit Delete
	Import Export
	OK Cancel

Note: Users can use the dynamic security watermark feature to better protect PDF files from unauthorized duplication. The PDF file protected by dynamic security watermark will be saved in Foxit protected PDF format and can only be opened by Foxit products.

4 Adding Watermark

To add a new watermark, please do the following:

- Open the Security Watermark Management, select a profile you created and click **Add** to add watermarks to the profile.
- Name the watermark in the Name field.
- Type the watermark's content in the text box and set the font, size, color, underline, and alignment.

Note: you can only set text as watermark.

 In the Dynamic text, you can select the option as needed to show the dynamic security watermark.

Select dynamic variable: show the current document information dynamically and multiple text are available at the same time.

Content ID: shows the content ID of the current document.

Document Title: show the current document title.

Author: show the author of the current document.

Current User: show the current user who is reading the document.

Date: show the current system date when opening the document.

Day: show the current system day when opening the document.

Month: show the current system month when opening the document.

Year: show the current system year when opening the document.

Time: show the current system time when opening the document.

Hour: show the current system hours when opening the document.

Minute: show the current system minutes when opening the document. **Second**: show the current system seconds when opening the document.

- Set the appearance by choosing the rotation degree and the opacity. You also have the option to select the scale relative to the target page.
- Set the vertical and horizontal distance between the target page and the watermark.
- Choose the page range to display the watermark. You can choose to display the watermark for all pages in rage, even pages only or odd pages only in the subset list.
- Preview the watermark in the right pane.
- Click **OK** to finish it.

Edit Security Watermark	×
Name: Highly Confidential Source: Text: HIGHLY CONFIDENTIAL Font: System V Size: 48 V T E E E	Preview
Dynamic text: Select dynamic variable▼ Appearance Rotation: 0.45° C None Opacity:	TDENTIAL
Position Vertical Distance: 0.00 Horizontal Distance: 0.00 Page Range Options	HGHLYCONFIDENTIAL
All Pages Pages: Pages rom: 1 to: 1 Subset: All pages in range	
	OK Cancel

Editing or Deleting Watermark

Editing a Watermark

- Open the Security Watermark Management and select a watermark you want to edit.
- Click **Edit** to open the Edit Security Watermark dialog box.
- Start to edit the watermark, please refer to "Adding Watermark".
- Click **OK** to finish the operation.

Deleting a Watermark

- Open the Security Watermark Management and select a watermark you want to delete.
- Click **Delete** to remove the selected watermark.

Importing or Exporting Watermark

Importing a Watermark

- Open the Security Watermark Management and click Import.
- Choose a watermark with .xml format.
- Click Open.

Exporting a Watermark

- Open the Security Watermark Management and select a watermark you want to export.
- Click **Export** and choose a file type and location to save.
- The watermark will be exported as an .xml file or encoded file according to your choice. It can be integrated into AD RMS policy template and applied to the PDF files by Foxit Phantom PDF.

Note:

1. If you want to integrate the watermark to a common policy template, please export it as an .xml file and add it to the template by Phantom PDF directly.

2. If you want to integrate the watermark to an official policy template, please export it as an encoded file (.txt format) and integrate it into the template by AD RMS Scripting API Architecture. Then you can import the template and apply it to PDFs by PhantomPDF. (Please click <u>here</u> to see the example and use the value of "appData.Name" and "appData.Value" in the exported encoded file.)

Chapter 5 - FAQ

1. In the SharePoint environment, do we need to perform iisreset after installing the Foxit PDF Protector?

Yes. Foxit PDF Protector will not work immediately when it is installed. Please perform **iisreset** to ensure that the SharePoint server invokes Foxit PDF Protector.

2. Why is the PDF downloaded from the SharePoint Document Library still unprotected after installing the Foxit PDF Protector?

First, check that the IRM protection rules have been configured in the **SharePoint Document Library**. For example, ([Library Name]->Setting->Information Rights Management Settings->Restrict permission to documents in this library on downloads).

Then, clear your browser's Temporary Internet Files. For example, (IE8: Internet Options->General->Delete->check Temporary Internet files->click delete).

3. Why doesn't the Foxit PDF Protector work after being used for some period of time?

Because that you can only use the Free Trial version for 30 days. If you want to continue using the Foxit PDF Protector, please contact us by sending an email to <u>sales@foxitsoftware.com</u> to get the formal product license.

4. I got the authorized license file. How can I use it?

Please copy the license file to the same folder where you installed Foxit PDF Protector.

Note: Please ensure that all the users in the domain have the basic permission to "Read" and "Read & Execute", or the license file may not work.

Contact Us

Feel free to contact us should you need any information or have any problems with our products. We are always here, ready to serve you better.

 Office Address: Foxit Software Incorporated 39355 California Street Suite 302 Fremont, CA 94538 USA

- Sales: 1-866-680-3668
- Support & General: <u>Support Center</u> 1-866-MYFOXIT, 1-866-693-6948
- Website:
 www.foxit.com
- *E-mail:* Marketing <u>marketing@foxit.com</u>