

Foxit[®]



User Manual

Foxit[®] PDF

Secure RMS Protector



Microsoft[®] Partner

Silver Independent Software Vendor (ISV)

©2012 Foxit Corporation. All rights reserved.

Copyright © 2012 Foxit Corporation. 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 for MOSS 2007	6
Corresponding permissions of Foxit Reader and MOSS	7
Installing Foxit PDF Secure RMS Protector on a SharePoint Server	7
View and Manage Event Logs of Foxit PDF Secure RMS Protector	10
Check the version of Foxit PDF Secure RMS Protector	12
Editing Wrapper Content	13
Configuring AD RMS to Work with SPS-SRV	13
For MOSS 2007	14
To add SPS-SRV to Local Intranet.....	14
To add SPS-SRV to the AD-RMS Certification Pipeline.....	14
To activate Information Rights Management in Office SharePoint Server 2007.....	14
To restrict permissions using AD-RMS.....	15
For MOSS 2010	15
To add SPS-SRV to Local Intranet.....	15
To add SPS-SRV to the AD-RMS Certification Pipeline.....	15
To activate Information Rights Management in Office SharePoint Server 2010.....	16
To restrict permissions using AD-RMS.....	16
Working with Foxit PDF Secure RMS Protector	16
For MOSS 2007	16
To add the domain user to SharePoint site.....	16
To set the group permission in SharePoint site.....	17
To restrict the print permissions using RMS	19
For MOSS 2010	21
To add the domain user to SharePoint site.....	21
To set group permission in SharePoint site.....	22
To restrict the print permissions using RMS	24
Chapter 3 - For Exchange 2010	27
Getting Started	27
System requirements	27
Corresponding permissions of Foxit Reader and Exchange	27
Installing Foxit PDF Secure RMS Protector on an Exchange Server	27
Uninstalling Foxit PDF Secure RMS Protector	29
Check the version of Foxit PDF Secure RMS Protector.....	30

Editing Wrapper Content	31
Configuring AD-RMS to Integrate with Exchange Server 2010 in a Single Forest	31
To register a service connection point	32
To give Exchange servers permissions to access the server certification pipeline	32
To set up the Exchange Server super users group	33
To set InternalLicensingEnable true by ExchangeManagement Shell	33
Working with Foxit PDF Secure RMS Protector	34
Chapter 4 – Watermark Configuration Tool	38
Creating Profile	38
Adding Watermark	39
Editing or Deleting Watermark	40
Importing or Exporting Watermark	40
Chapter 5 - FAQ	42
Contact Us	43

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

Getting Started

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

System Requirements for MOSS 2007

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

System Requirements for MOSS 2010

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

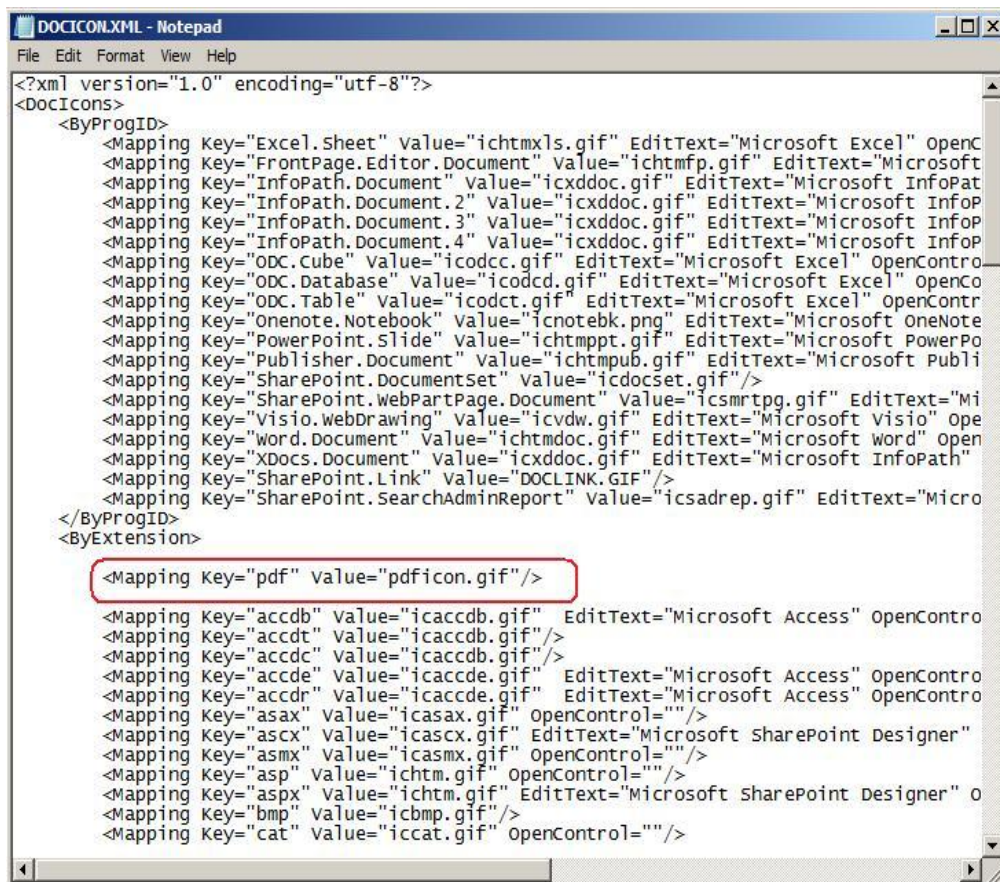
To install Foxit PDF Secure RMS Protector:

- 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 <http://www.foxitsoftware.com/images/icons/pdficon.gif>.
- For MOSS 2007,

1. Copy the downloaded.GIF 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 .gif file:
 <Mapping Key="pdf" Value="pdficon.gif"/>

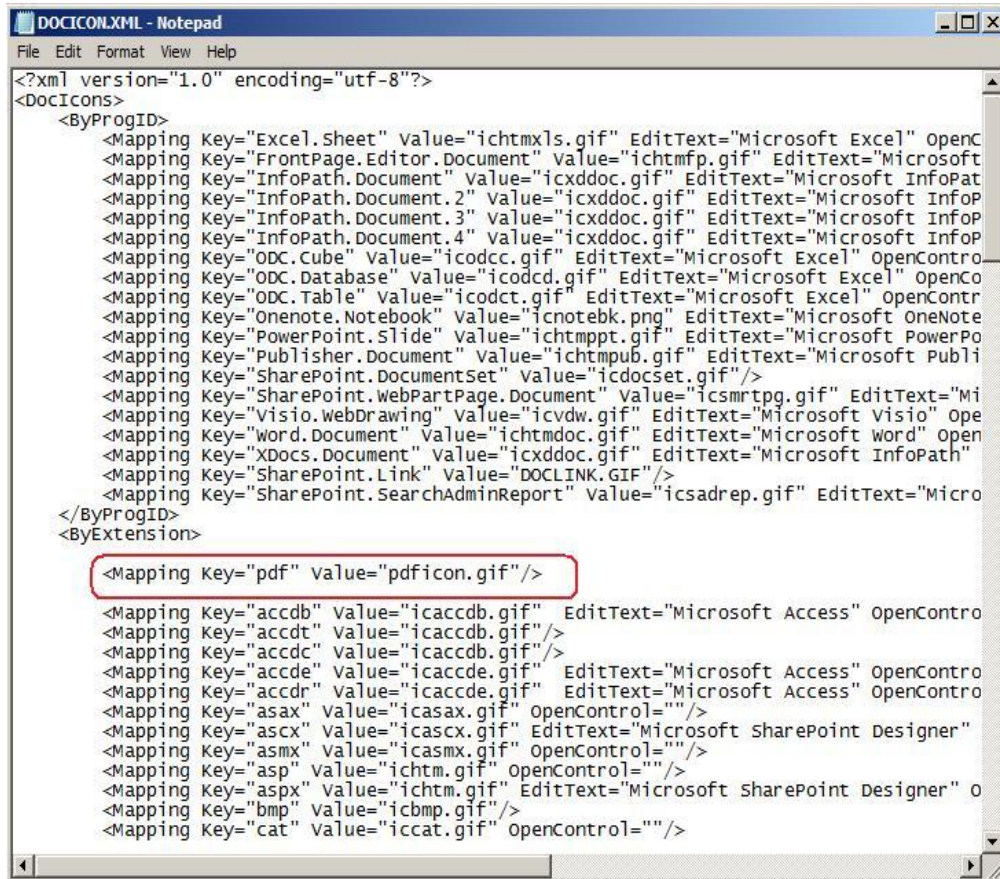


- c. Click Save on the File menu, and then quit Notepad.

- For MOSS 2010,
 1. Copy the downloaded.GIF 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 .gif file:

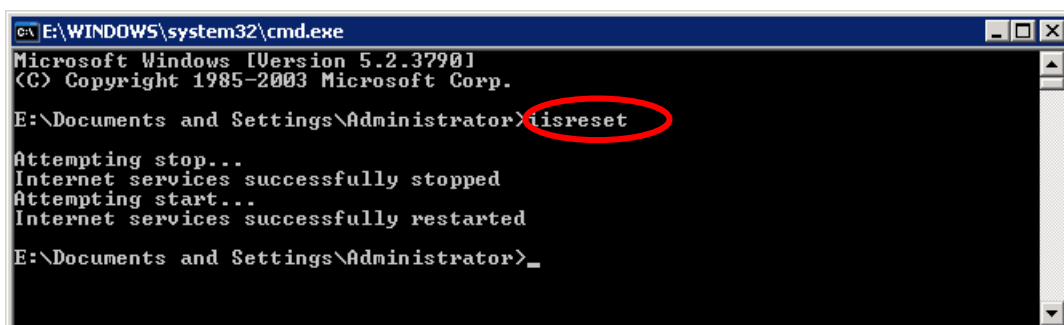
```
<Mapping Key="pdf" Value="pdficon.gif"/>
```



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

3. 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



- Click Finish button to complete removal.

View and Manage Event Logs of Foxit PDF Secure RMS Protector

To view and save the log information of the Protector, please do as 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

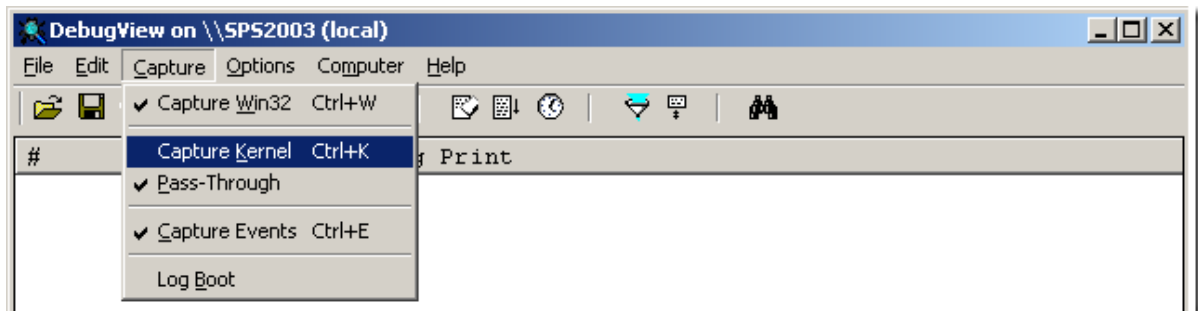
Data: 1

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.

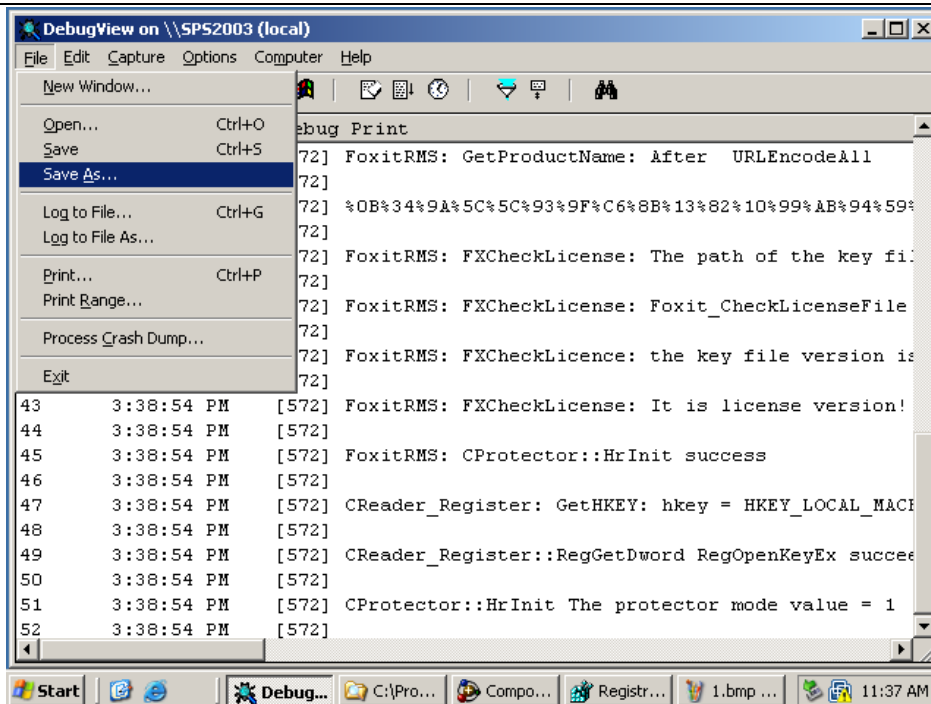
2. Download the **DebugView** tool from the following link and run it.

<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.



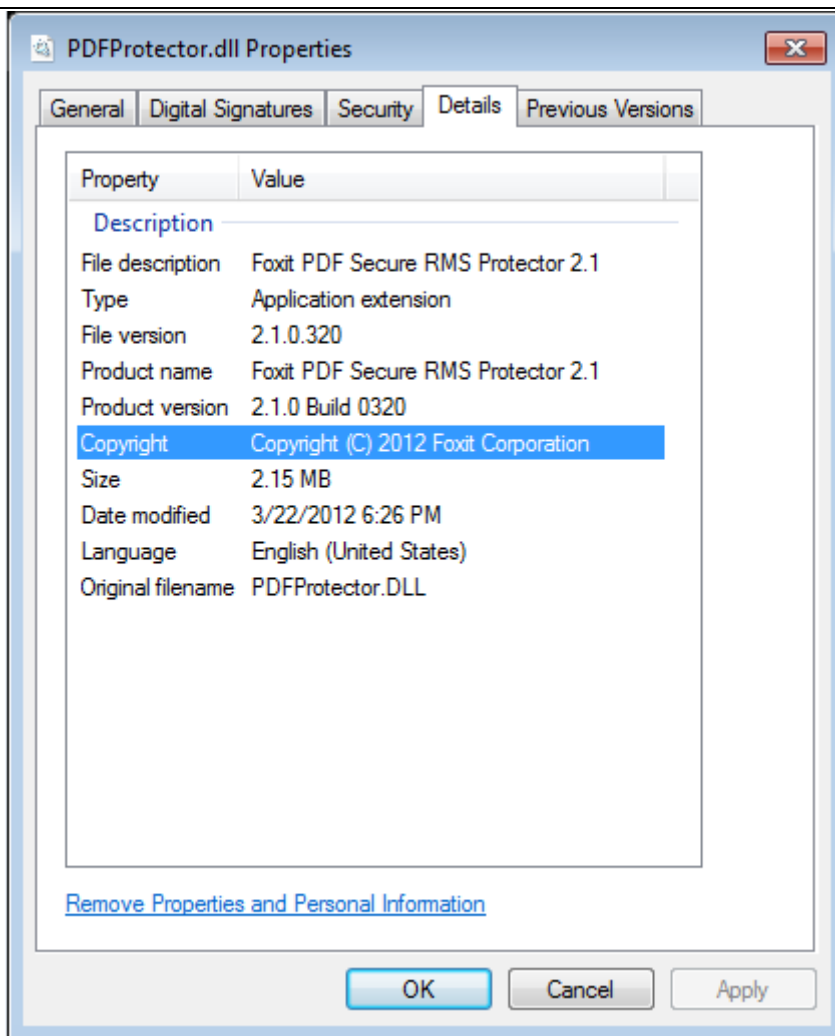
3. Perform an iisreset command (Please refer to [Perform an iisreset](#)), and you will be able to see the related log information now. The log information can be saved as a .txt file.



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:



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**.
9. 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**.

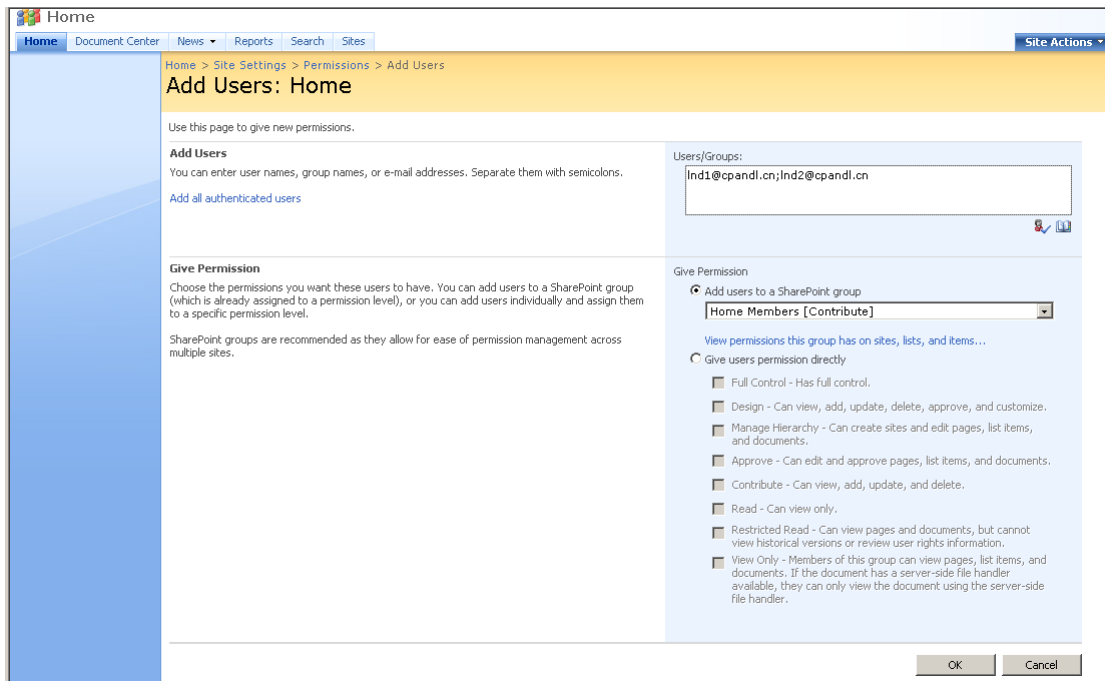
Working with Foxit PDF Secure RMS Protector

For MOSS 2007

To add the domain user to SharePoint site

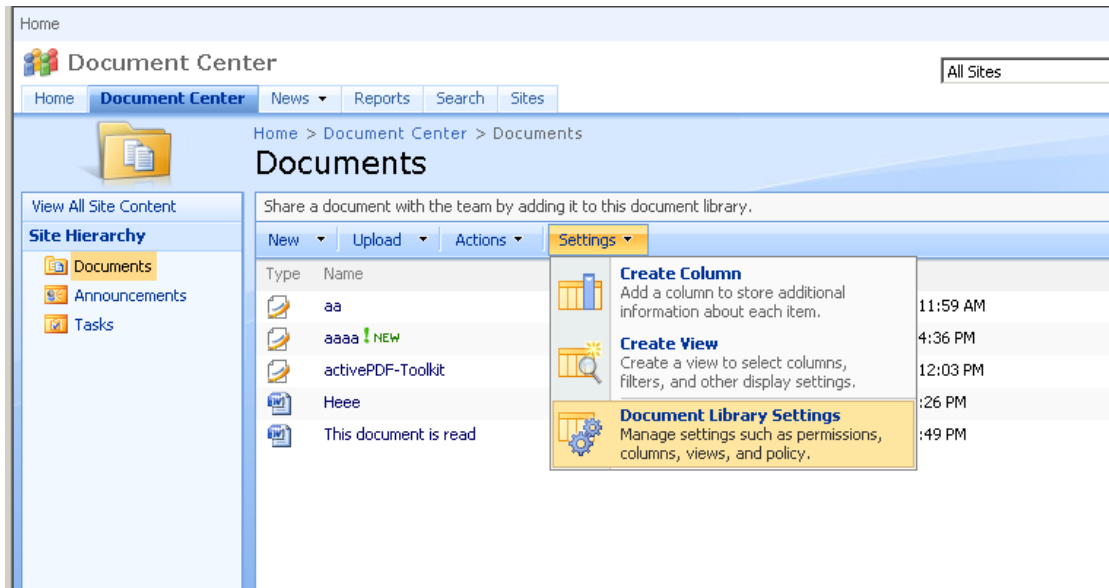
- In the same Office SharePoint Server 2007 site, click **Home**.

- 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.

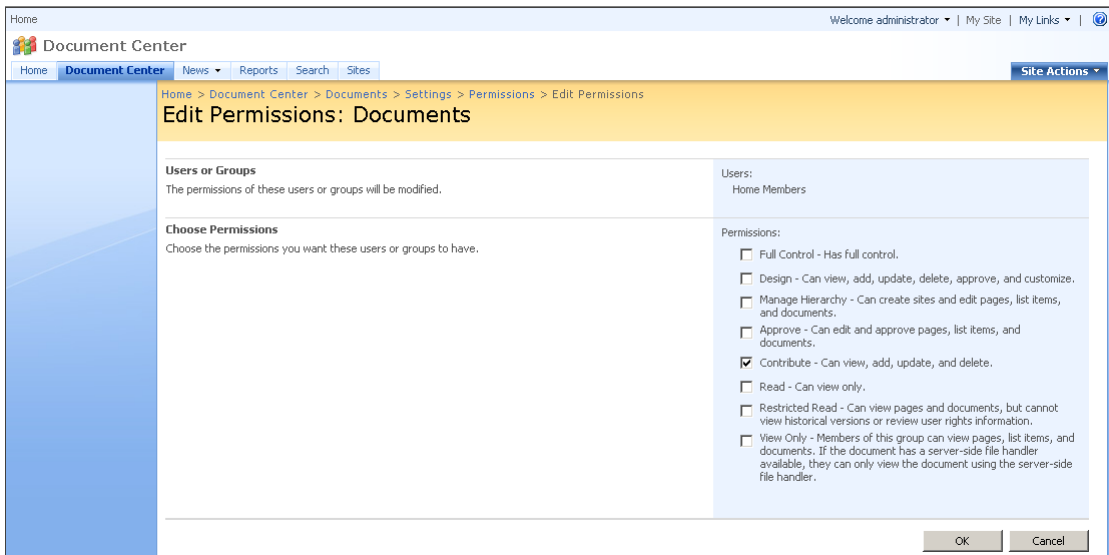


To set the group permission in SharePoint site

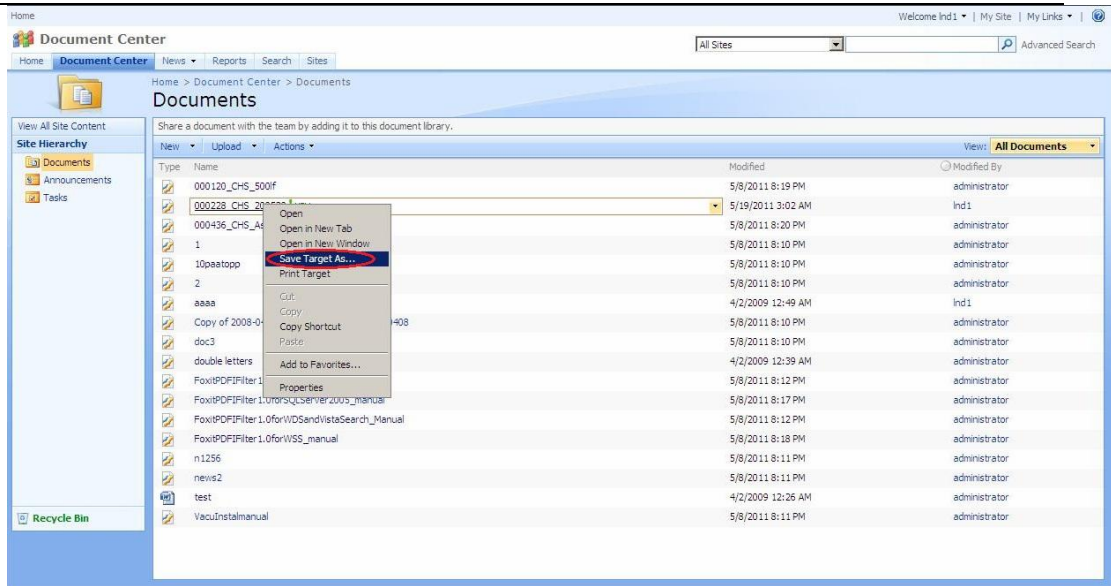
- Navigate to the **Documents** page, log on as administrator@cpandl.com, clicking the **Settings** drop-down box and select **Document Library Settings**.



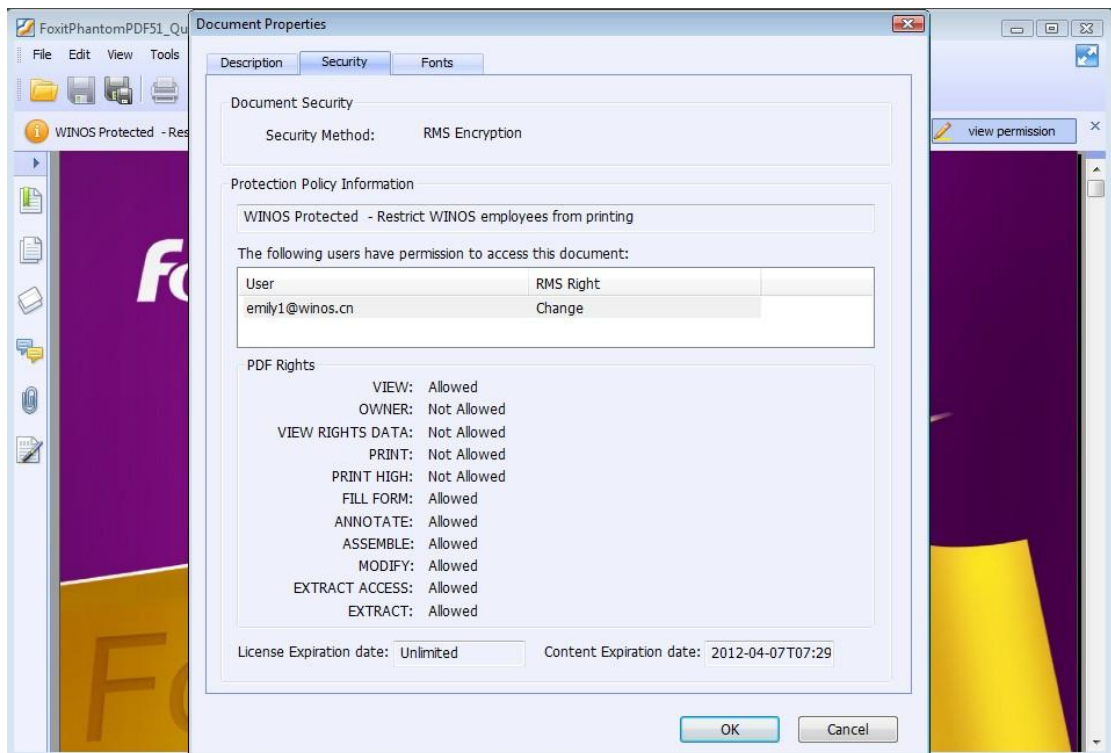
- Click **Permissions for this document library** under Permissions and Management on the Customize Documents page.
- Please click **Home Members** on “Permissions: Documents” page.
- Please choose the permission you need, for example, you can choose the **Contribute-Can view, add, update, and delete**.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



- Return to **Documents** page, log on as lnd1@cpandl.com, to download a PDF file to your host.



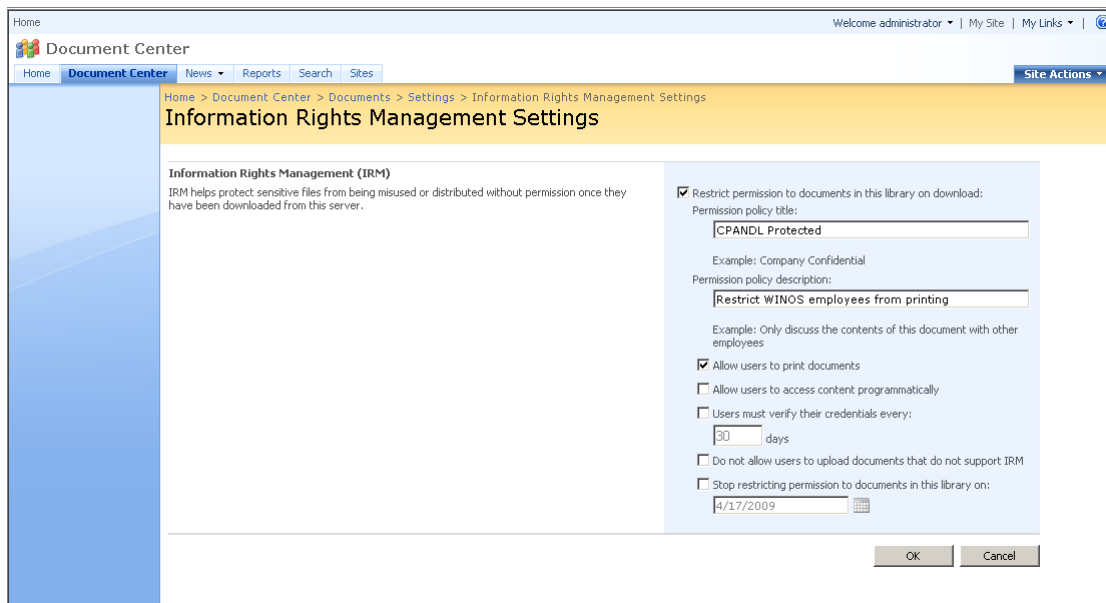
- Open the download PDF file by Foxit Reader, and left-click **View Permission** to see the **RMS Right**.



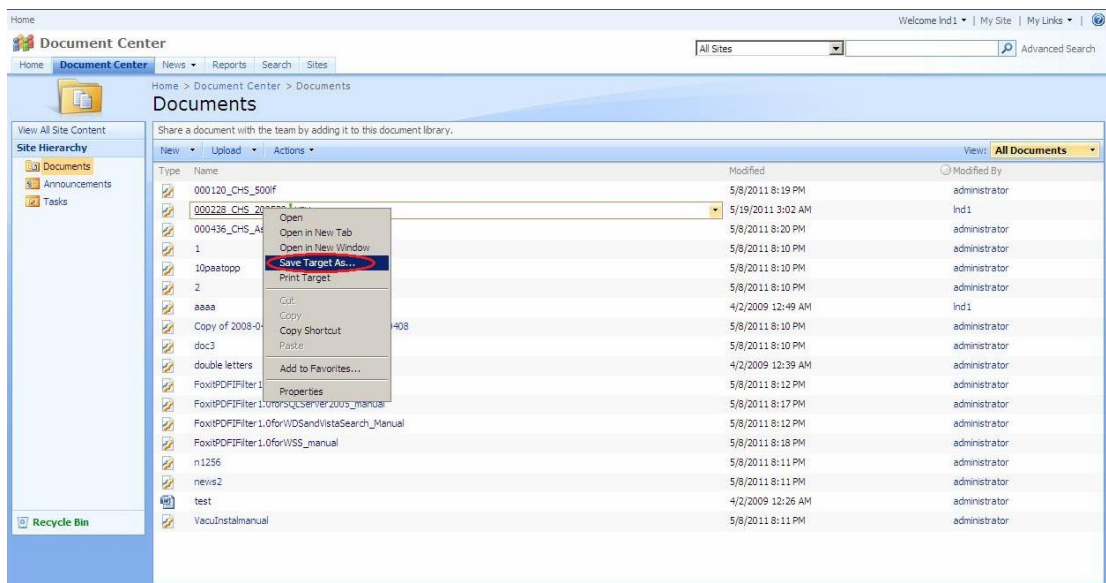
To restrict the print permissions using RMS

- 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**.

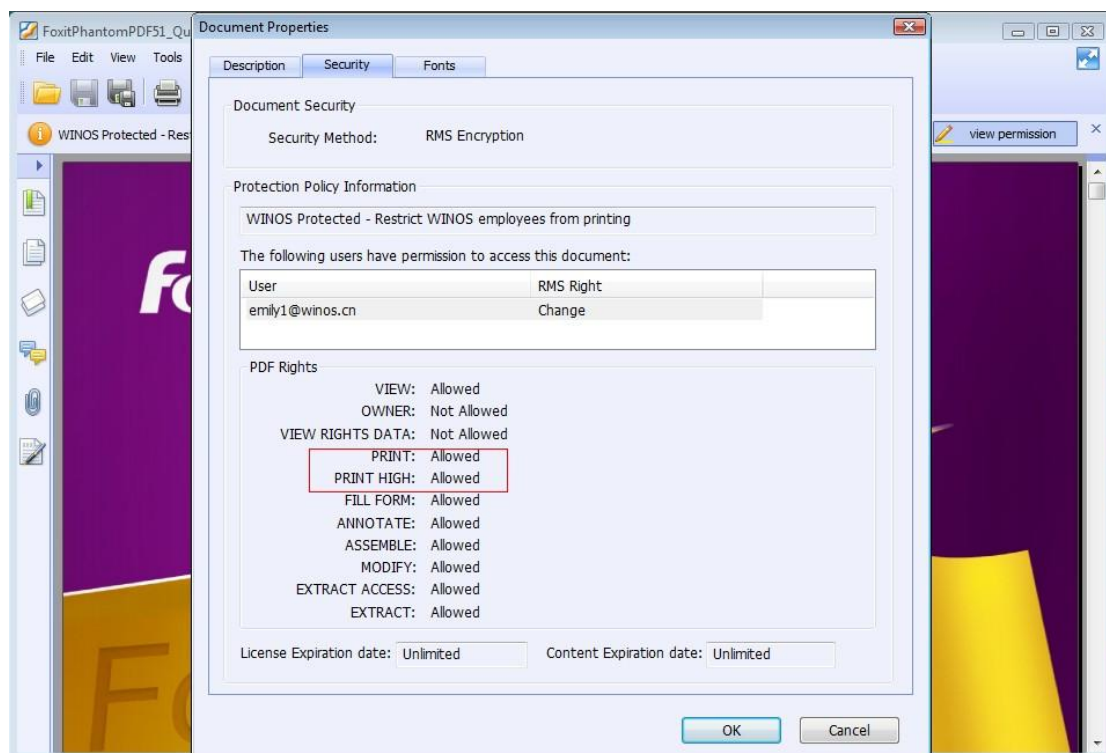
- On settings page, choose **Information Rights Management** under Permissions and Management.
- Choose **Allow users to print documents**, and then click **OK**.



- 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.



- 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.



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.



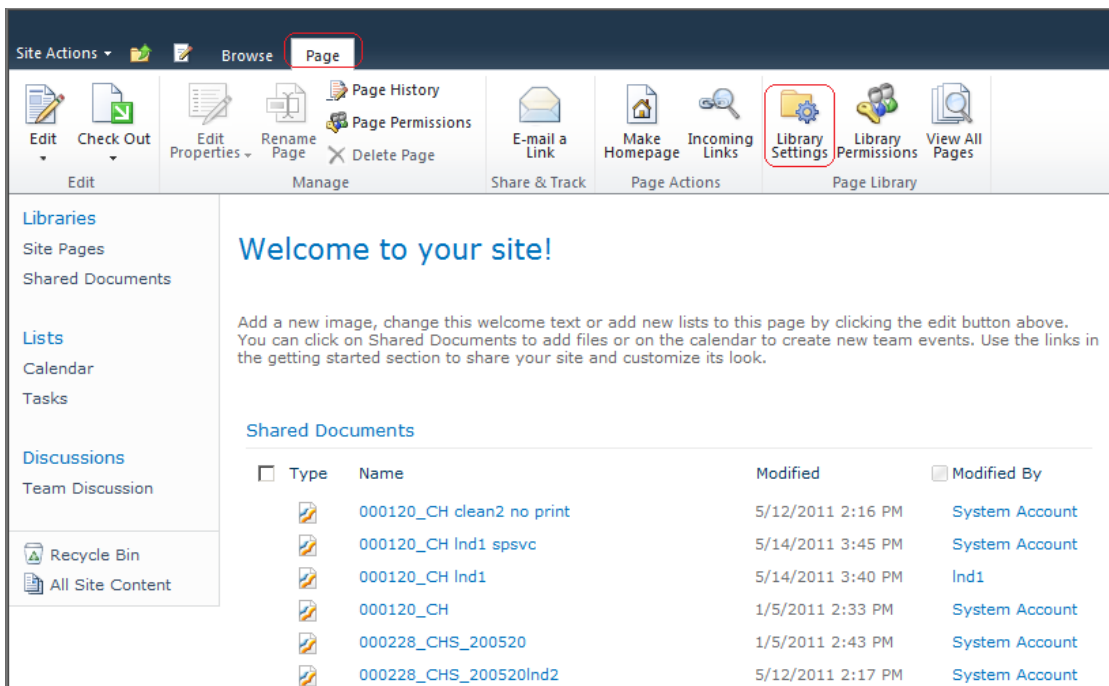
To set group permission in SharePoint site

Log on as CPANDL\Administrator.

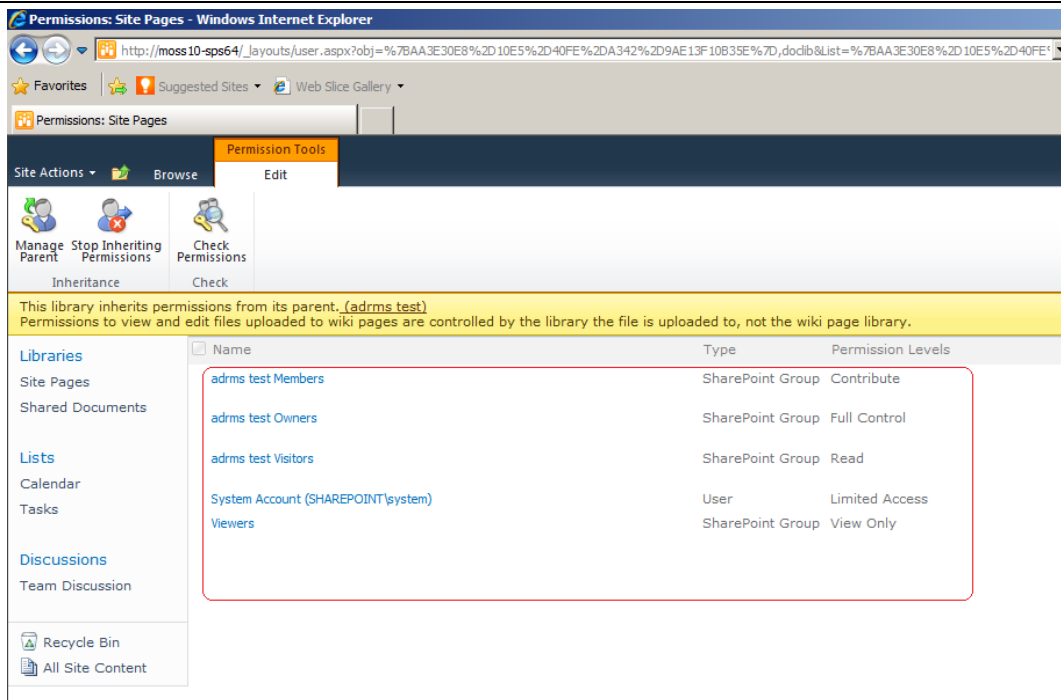
Click **Start**, and point to **All Programs**, and then click **Internet Explorer**.

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

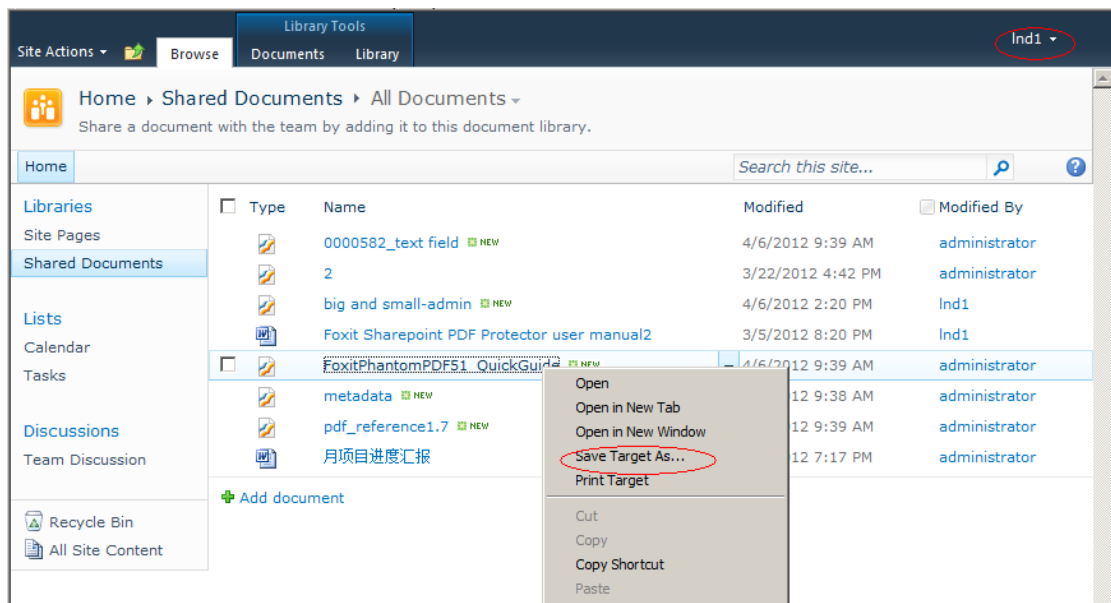
Click **Shared Documents** and **Library** page, then click **Library Settings** button.



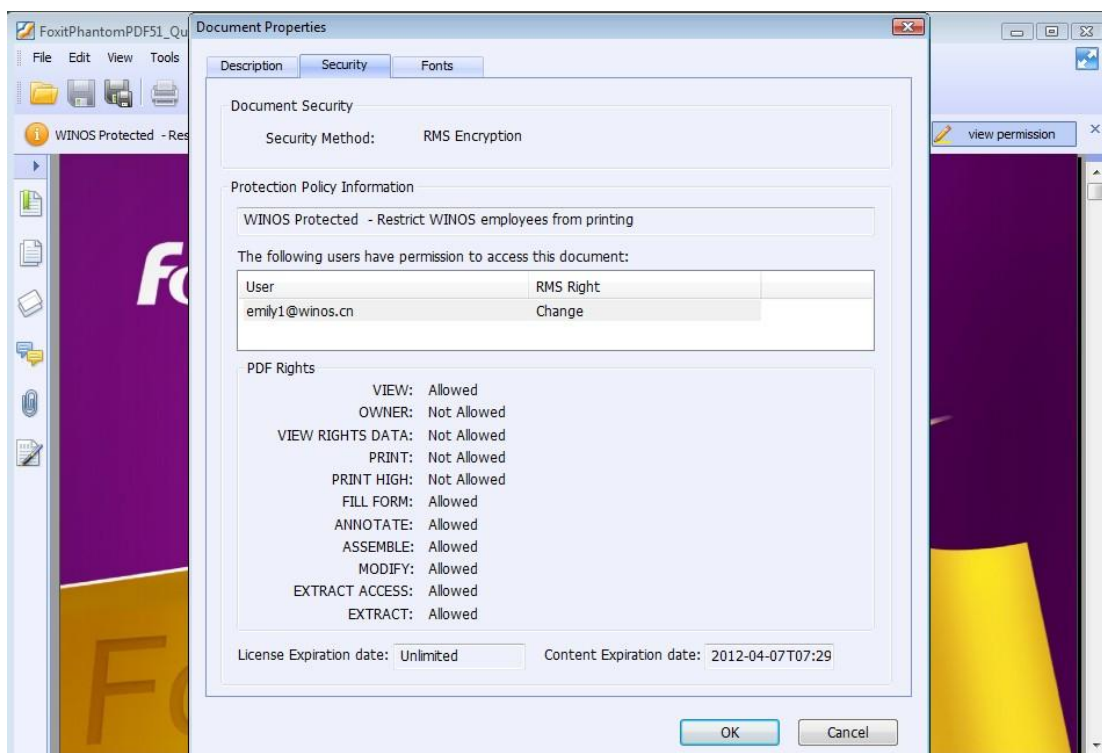
- Click **Permissions for this document library** under Permissions and Management on Customize Documents page.



- 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.

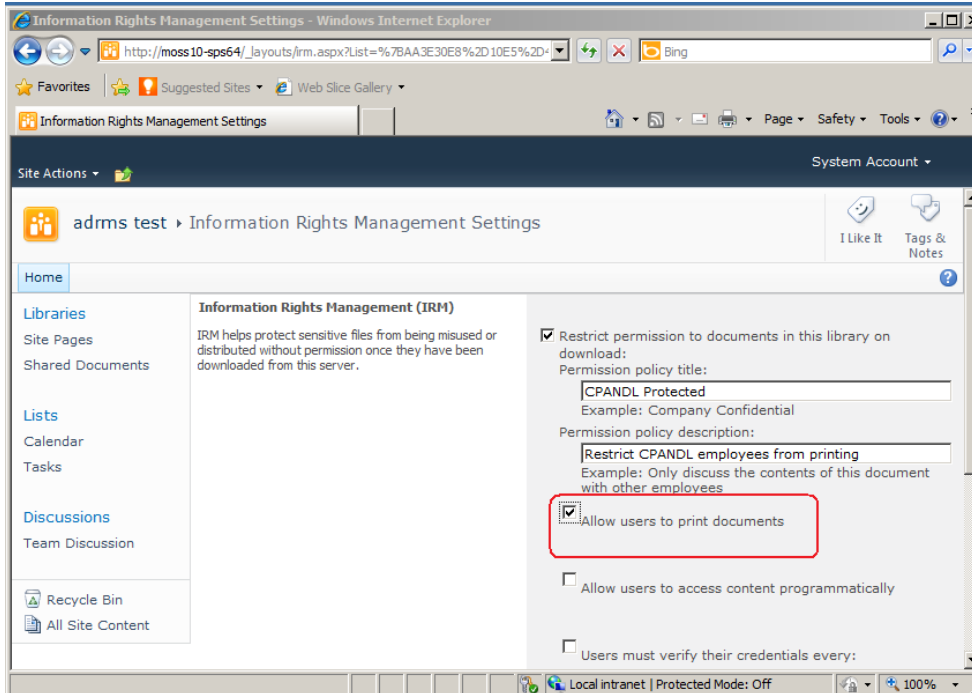


- Open the download PDF file by Foxit Reader, and left-click **View Permission** to see the **RMS Right**.

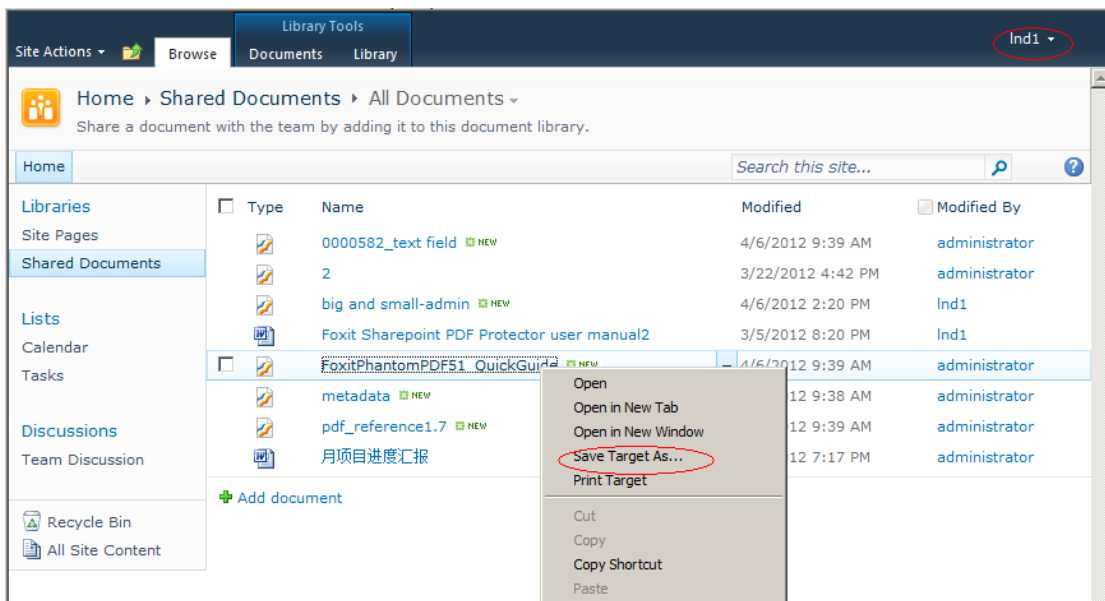


To restrict the print permissions using RMS

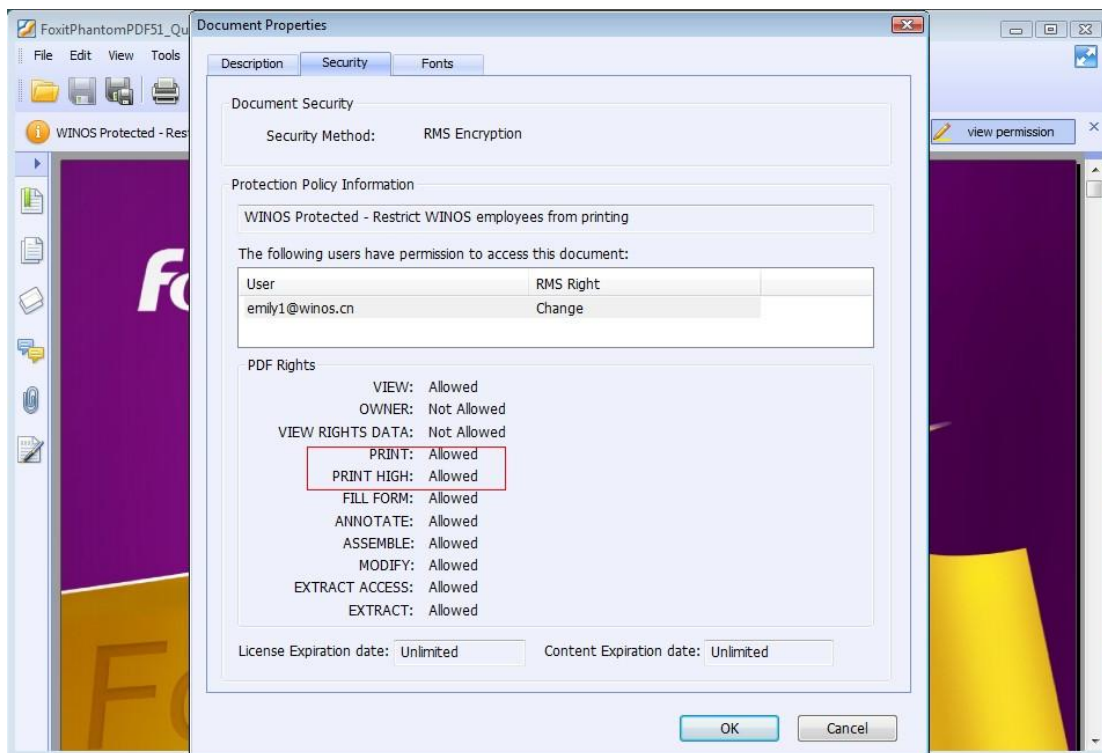
- In the same Office SharePoint Server 2010 site, click Home.
- Click **Shared Documents** and **Library** page, then click **Library Settings** button.
- On the settings page, choose **Information Rights Management** under Permissions and Management.
- Choose **Allow users to print documents**, and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



- 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.



Chapter 3 - For Exchange 2010

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

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 2003 with SP1	Active Directory, Domain Name System (DNS)
ADRMS-DB	Windows Server 2003 with SP1	Microsoft SQL Server™ 2005
Exchange Server 2010 Such as named EX01	Windows Server 2008 with SP2 or Windows Server 2008 R2	Exchange Server 2010 and has been added this Server to DC
Client	Win7	Client , Outlook 2010

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 ,restart IIS, MExchangeTransport, msftesql-Exchange:
1. Click Start > Run > type "cmd" in the Open line> click OK, and execute the following commands:

```
net stop MExchangeTransport
```

```
net start MExchangeTransport
```

```
net stop msftesql-Exchange
```

```
net start msftesql-Exchange
```

```
net start MExchangeSearch
```

```
iisreset
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.CPANDL>net stop MExchangeTransport
The Microsoft Exchange Transport service is stopping.
The Microsoft Exchange Transport service was stopped successfully.

C:\Users\Administrator.CPANDL>net start MExchangeTransport
The Microsoft Exchange Transport service is starting..
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 MExchangeSearch
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 stopped
Attempting start...
Internet services successfully restarted

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

2. Close the windows.

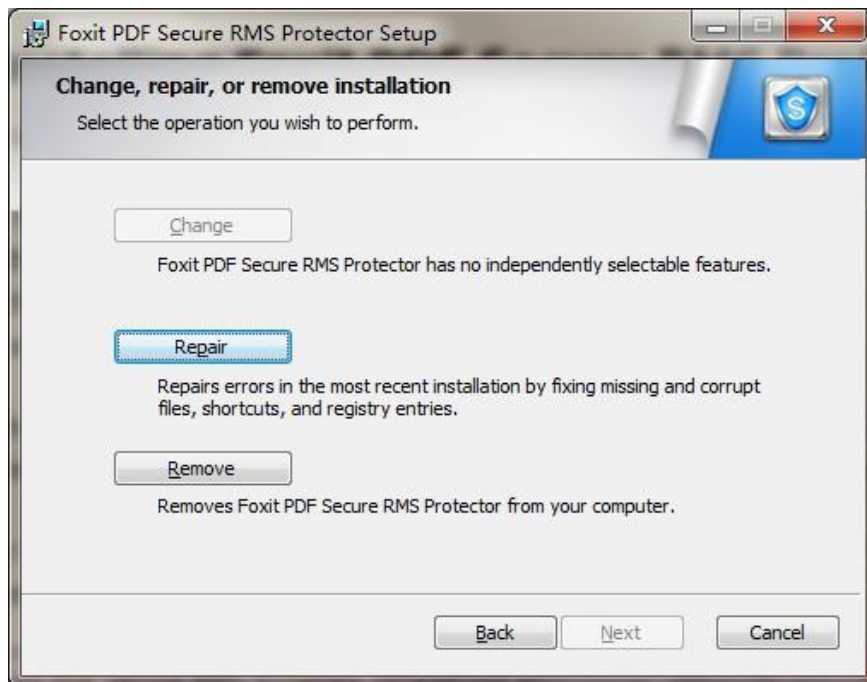
Uninstalling Foxit PDF Secure RMS Protector

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:

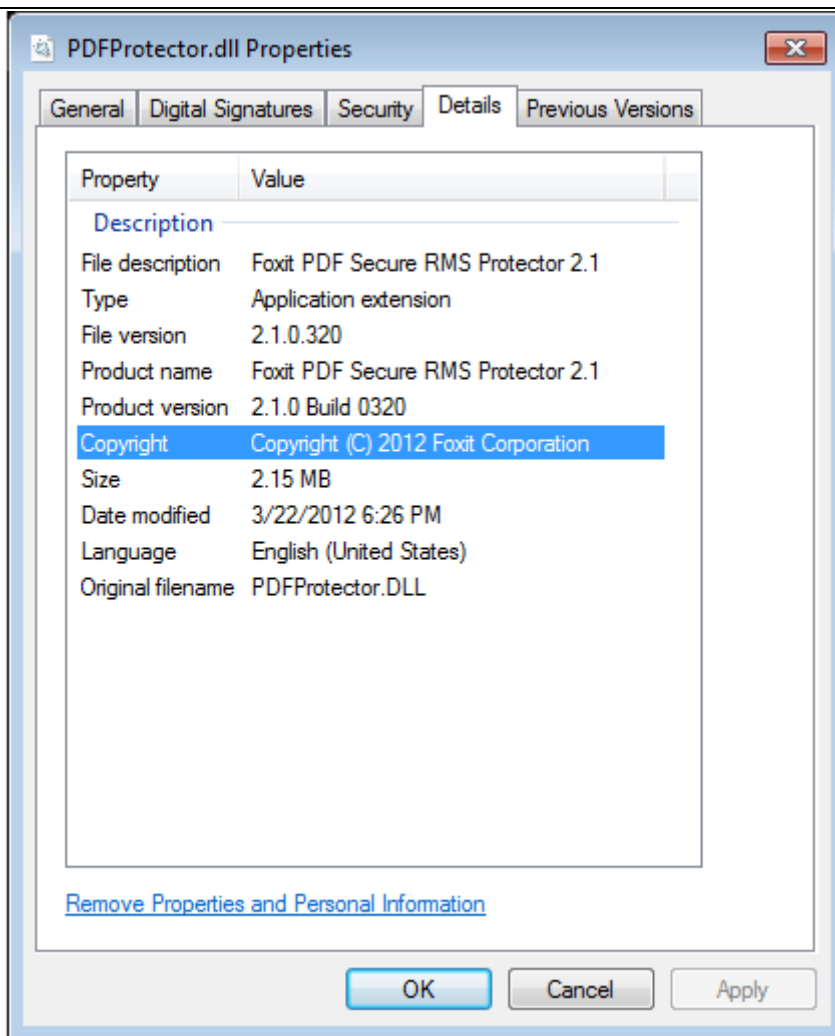
- In the Foxit PDF Secure RMS Protector dialog box, select Remove Foxit PDF Secure RMS Protector



- Click Next button to uninstall it completely.

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:



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 2010 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**.
8. 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.
5. 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 **EXO1**
2. Navigate to Start->All Programs->Microsoft Exchange Server 2010->Exchange Management Shell
3. Type "Get-IRMConfiguration"

```

Machine: EX01.cpandl.com
Tip of the day #47:
You can control which features are available to Outlook Web Access users h
pe:
Set-OwaVirtualDirectory "OWA (Default Web Site)" -ContactsEnabled $True -
VERBOSE: Connecting to EX01.cpandl.com
VERBOSE: Connected to EX01.cpandl.com.
[PS] C:\Windows\system32>Get-IRMConfiguration

InternalLicensingEnabled      : False
ExternalLicensingEnabled     : False
JournalReportDecryptionEnabled : True
OWAEnabled                    : True
SearchEnabled                 : True
TransportDecryptionSetting    : Optional
ServiceLocation              :
PublishingLocation            :
LicensingLocation             : <>

[PS] C:\Windows\system32>

```

4. Type " Set-IRMConfiguration -InternalLicensingEnable \$true" to enable licensing.

5. Type " Get-IRMConfiguration " again ,to check InternalLicensingEnalbe is true.

```

Machine: EX01.cpandl.com
Has one of your users asked you to recover their mobile device synchronization password? To return the user's password,
type:
Get-ActiveSyncDeviceStatistics -ShowRecoveryPassword
VERBOSE: Connecting to EX01.cpandl.com
VERBOSE: Connected to EX01.cpandl.com.
[PS] C:\Windows\system32>Set-IRMConfiguration -InternalLicensingEnable $true
WARNING: The command completed successfully but no settings of 'ControlPoint Config' have been modified.
[PS] C:\Windows\system32>Get-IRMConfiguration

InternalLicensingEnabled      : True
ExternalLicensingEnabled     : False
JournalReportDecryptionEnabled : True
OWAEnabled                    : True
SearchEnabled                 : True
TransportDecryptionSetting    : Optional
ServiceLocation              :
PublishingLocation            :
LicensingLocation             : <>

[PS] C:\Windows\system32>

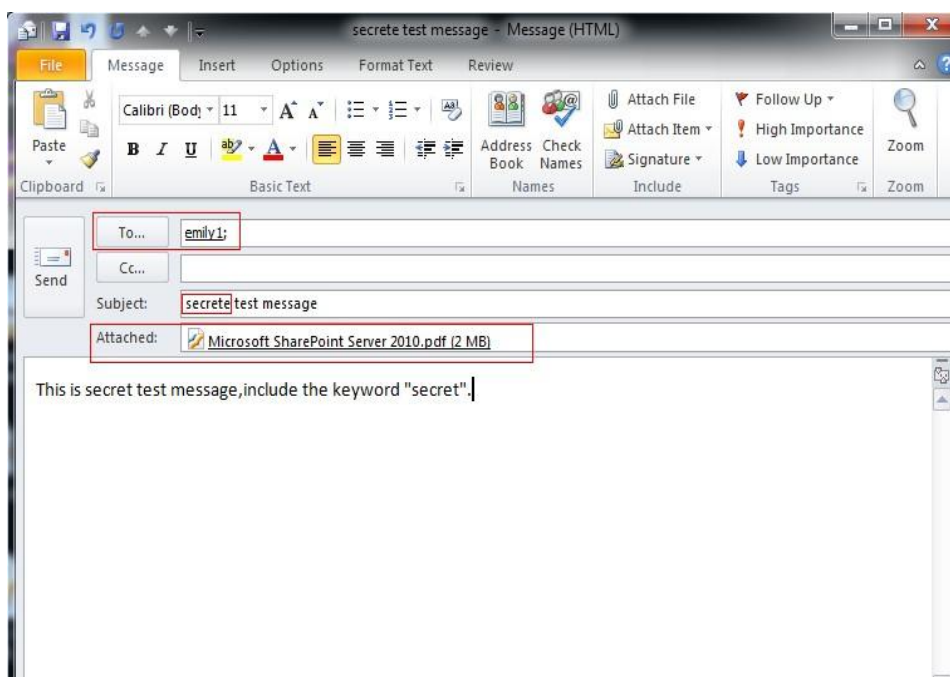
```

Working with Foxit PDF Secure RMS Protector

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"

```
Machine: EX01.cpandl.com
Exchange team blog: get-exchlog
Show full output for a cmd: <cmd> ! format-list
Tip of the day #52:
Want to get a list of the backup status of all mailbox databases in your organization? Type:
Get-MailboxDatabase -Status ! Format-Table Name, Server, *Backup*
How about just the mailbox databases on a specific server? Type:
$Databases = Get-MailboxDatabase -Server <Server Name> -Status
$Databases | Format-Table Name, *Backup*
VERBOSE: Connecting to EX01.cpandl.com
VERBOSE: Connected to EX01.cpandl.com.
[PS] C:\Windows\system32>New-TransportRule -Name "Test Transport Rule for Encryption" -Enabled $true -SubjectOrBodyContainsWords "secret" -ApplyRightsProtectionTemplate "Do Not Forward"
Name State Priority Comments
----
Test Transport Rule for Encryption Enabled 0
[PS] C:\Windows\system32>
```

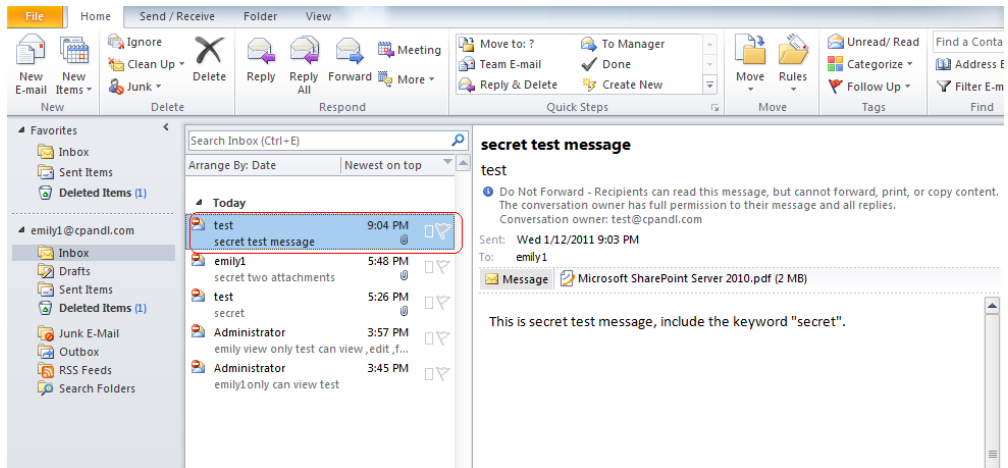
4. Log on as CPANDL\test to Client, and open Microsoft Outlook 2010, new an Email (for example, send an e-mail to emily1@cpandl.com). The Email includes the PDF attachment.



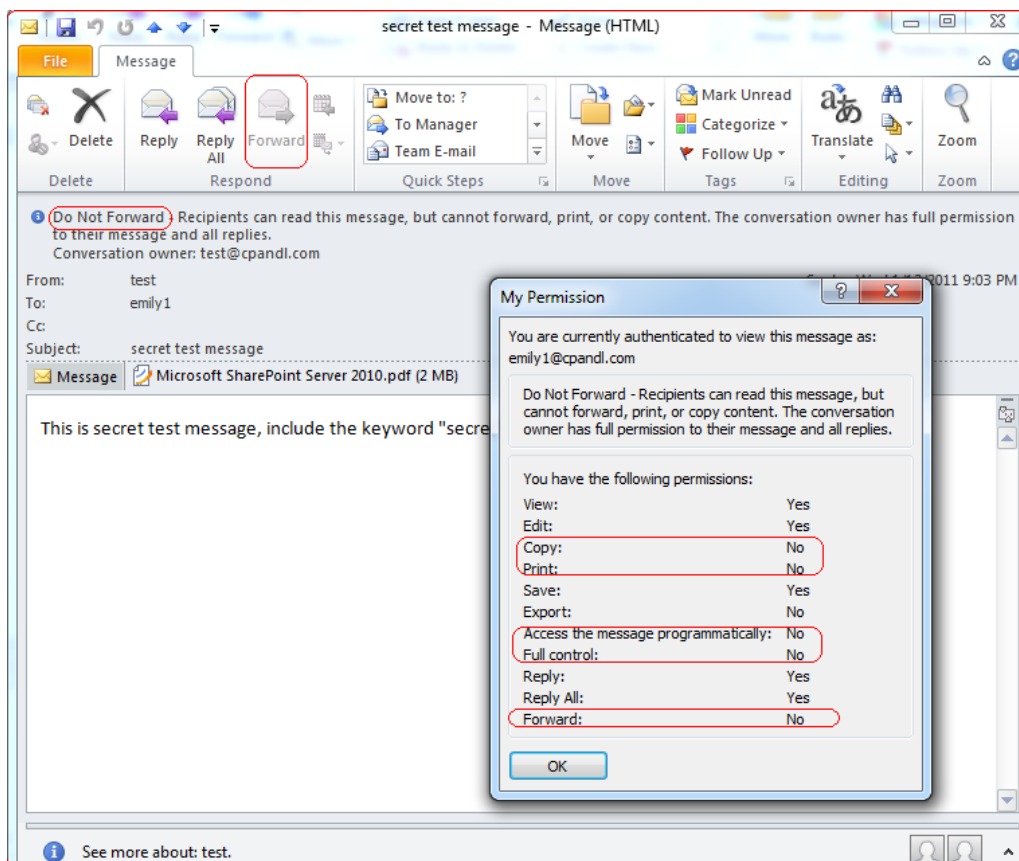
And then click **Send**.

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

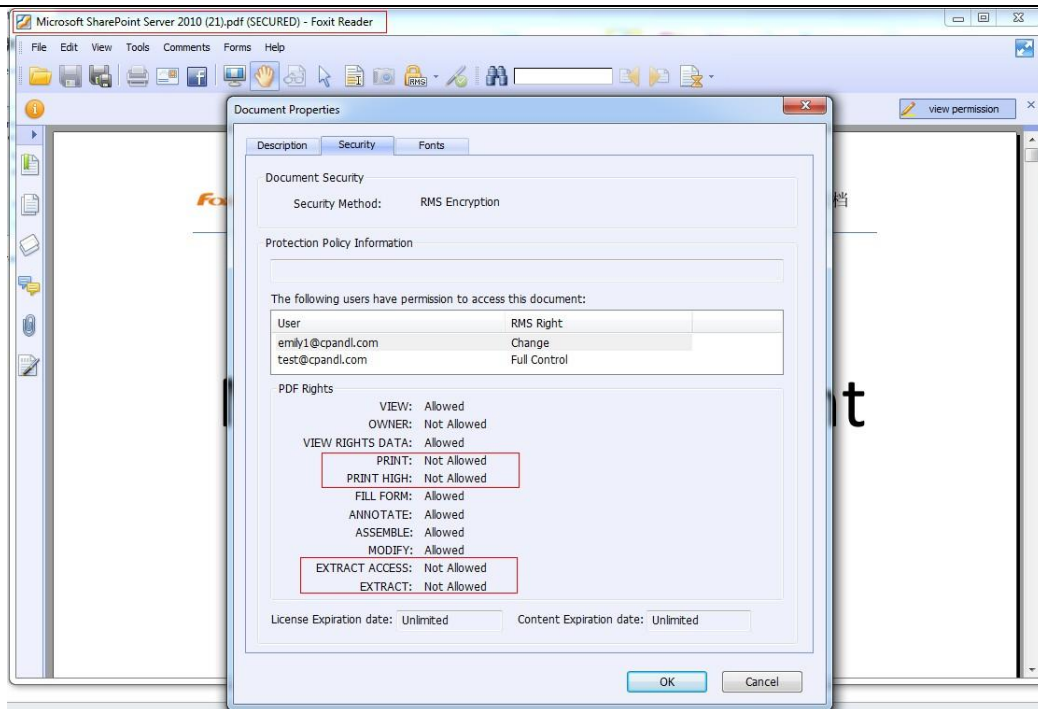
6. Open Microsoft Outlook 2010. In the inbox, we can see the email which has been tested to send.



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.




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



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.

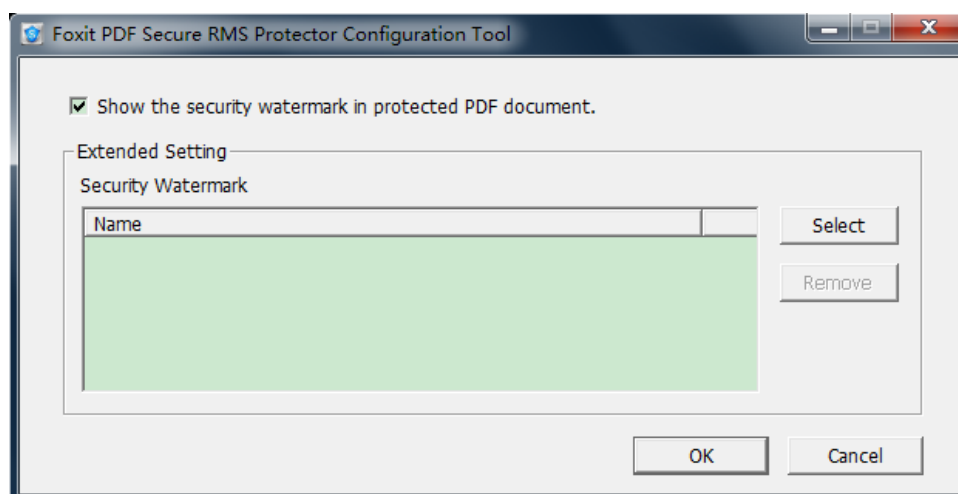
The watermark configuration tool will pop up after finishing the installation or you can double-click the icon  on desktop to open it.

Creating Profile

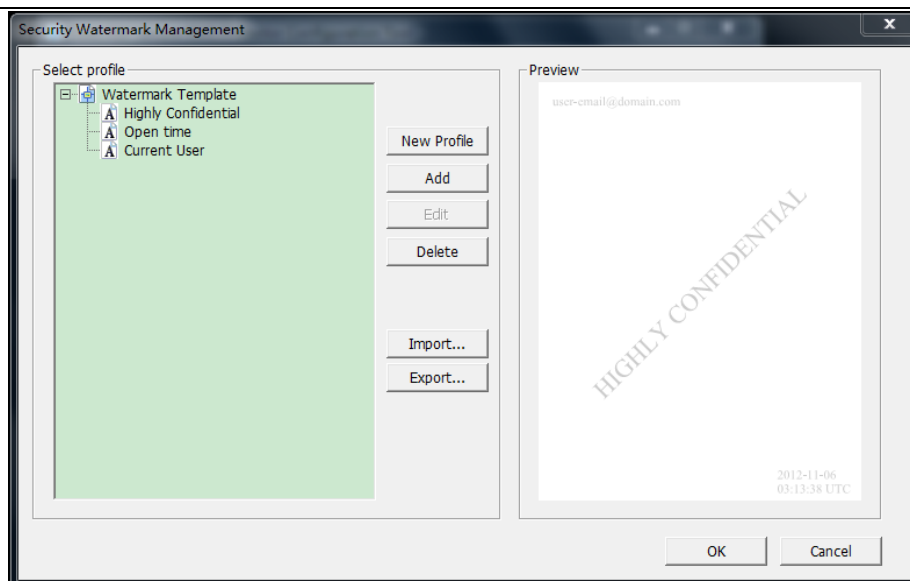
Before adding a watermark, you should create a profile first. The application will apply all of the watermarks in the profile to a PDF.

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.”



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



Adding Watermark

To add a new watermark, please do the following:

- Open the Security Watermark Management and select a profile you created and click **Add** to add watermarks in the profile.
- Title the watermark's name.
- 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.

- Choose the Dynamic text. Whenever any reader opens the file, the watermark will show the current document information dynamically and you can use multiple texts at the same time.

Document Title: show the current document title.

Author: show the author of 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.

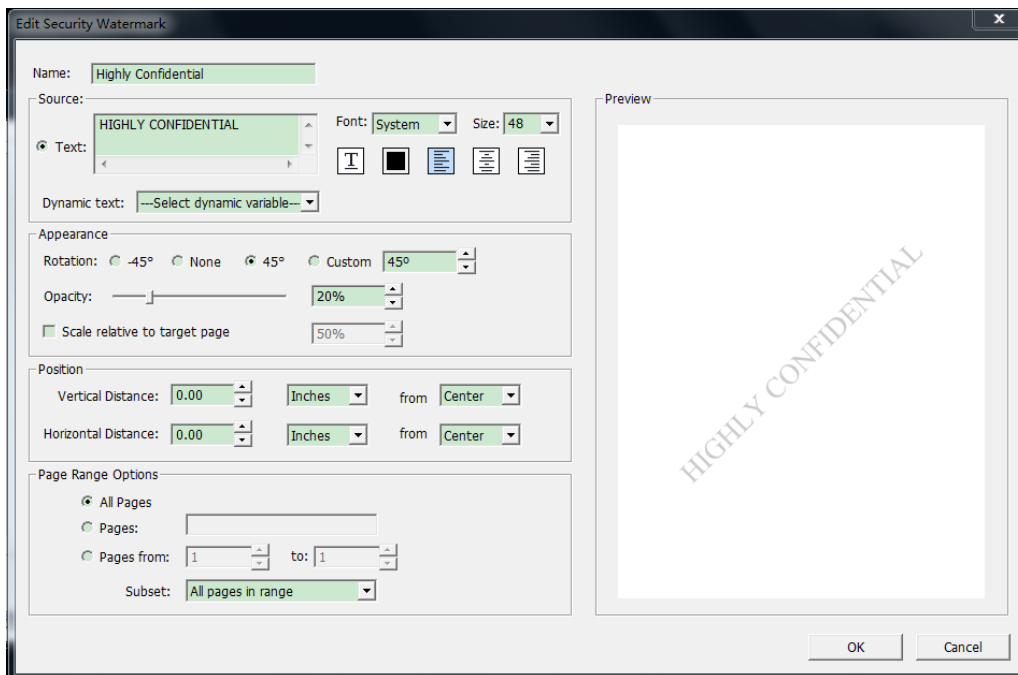
Hour: show the current system hours when opening the document.

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 play the watermark. You have several options for page range via clicking the right items in the subset list.
- Preview the watermark in the right pane.
- Click **OK** to finish it.



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 Create 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 [here](#) 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 sales@foxitsoftware.com 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 Corporation
42840 Christy Street. Suite 201
Fremont CA 94538
USA
- **Mailing Address:**
Foxit Corporation
42840 Christy Street. Suite 201
Fremont CA 94538
USA
- **Sales:**
1-866-680-3668 (24/7)
- **Support:**
1-866-MYFOXIT or 1-866-693-6948(24/7)
- **Fax:**
510-435-9288
- **Website:**
www.foxitsoftware.com
- **E-mail:**
Sales and Information - sales@foxitsoftware.com
Technical Support - support@foxitsoftware.com
Marketing Service - marketing@foxitsoftware.com